COBIT™
導入ツールセット

1998年4月
第2版

COBIT運営委員会および
情報システムコントロール財団

COBITの使命：
ビジネスマネジャーおよび監査人が日々利用するために
権威のある，最新の，国際的に一般に認められた
情報テクノロジーコントロール目標の体系を
調査し，開発し，公表し，推進すること

目　次

情報システムコントロール財団
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
電話:　+1.847.253.1545
Fax:　+1.847.253.1443
E-mail:　research@isaca.org
Web site:　www.isaca.org

ISBN　0-9629440-7-6 (導入ツールセット)
ISBN　0-9629440-3-3 (CD-ROM 付き 5 分冊)

印刷：アメリカ合衆国

導入ツールセットの紹介

1996 年，Control Objectives for Information and Related Technology (COBIT) の歴史的に画期的な紹介は，情報技術(IT)の統治とコントロール実務のための一般に適用可能で認められた枠組みを情報技術担当者へ与えた。

COBIT の第一の目的は，世界中の組織に IT 統治のための明確な方針とよい実務を提供することである。それは上級マネジメントが IT 関連リスクを理解し管理するための助けとなる。マネジメント，ビジネスプロセスオーナー，ユーザおよび監査人に，IT 統治の枠組みと詳細なコントロール目標のガイドを提供することにより，COBIT はこの目的を果たしている。

組織は自然にグループ化されたプロセスを通じて IT 資源を管理すべきであるという目標を達成するために必要な情報を提供するために，COBIT は簡潔で実務本位を前提としてスタートした。COBIT は簡潔でビジネス指向的な階層にプロセスをグループ化する。それぞれのプロセスは IT 資源に関連づけられ，また情報に対する品質上，信託上，セキュリティ上の要求に関連づけられている。

COBIT はビジネス指向であるので，COBIT を使って IT コントロール目標を理解して，IT 関連のビジネスリスクを管理することは簡単である。すなわち，

- 「枠組み」の中であなたのビジネス目標とともに始めよう。
- 「コントロール目標」からあなたの企業に適切な IT プロセスおよびコントロールを選択しよう。
- あなたのビジネス計画から運用しよう。
- 「監査ガイド」を使ってあなたの手続および結果を評価しよう。

COBIT が公表されてすぐに，COBIT 運営委員会は「グローバルベストプラクティス」がどのように導入されたかという評価を開始した。この「導入ツールセット」はこの評価の結果である。迅速にかつ成功裡に COBIT を適用した組織から学んだ教訓を他の組織が使うためにツールセットに取り入れた。

これらの教訓には次のアドバイスが含まれている。上級マネジメントを早い段階からディスカッションに巻き込みなさい。(概要レベルおよび詳細レベルの両レベルで) 枠組みを説明できるようにしておきなさい。他の組織からの成功事例を引用しなさい。COBIT 運営委員会は，それらのキーポイントの説明を改善し，理想的な導入プロセスの段階毎の概要 (例示を含む) を示すことが求められた。したがって，この「導入ツールセット」は次の項目を含んでいる。

- 「経営者のため要約」
- 「経営者のため概要」
- サンプルメモとプレゼンテーションを含む導入ガイド
- マネジメント理解度診断書と IT コントロール診断書
- COBIT 導入を説明した 8 つのケーススタディ

- **よく尋ねられる質問とその回答**
- COBIT **の導入用，販売用のプレゼンテーション・スライド**

COBIT をあなたの組織へどのように導入すべきか

紹介

COBIT は情報技術(IT)資源の管理とコントロールのための，一般に認められた実務指針を提供する。COBIT はマネジメント，ユーザ，監査人（あるいは評価や査定を行う人）という3種類の利用者を対象として設計された。

- マネジメントにとって　－　COBIT は「しばしば予測不可能な IT 環境でのリスクとコントロールの投資のバランスを知ること」に役立つ。
- ユーザーにとって　－　COBIT は「内部あるいは第三者機関から提供される IT サービスのセキュリティとコントロールに対する保証を獲得すること」に役立つ。
- 監査人にとって　－　COBIT は「IT の内部統制についてのマネジメントに対する監査人の意見に十分な根拠を与えること，および革新的なビジネスアドバイザーになること」に役立つ。

さらに，すべての利用者は COBIT を自己評価のガイドとして利用することができる。

組織のある機能分野は COBIT を利用することによって効果を得ることができる。マネージャは IT 投資の意思決定を指導し，IT 資源から最適な結果が得られることを保証するために，COBIT を利用することができる。COBIT の利用により，ユーザは IT サービスがビジネスプロセスを十分に支援しているという保証を得ることができる。監査人にとって，COBIT はレビューと検証の規準として，また枠組みの利用を通じて，監査の有効性と効率性を向上させる方法として，非常に有用である。しかしながら，結論として，COBIT はトップダウンプロセスとして始める必要はない。COBIT はボトムアップ主導で導入することが可能である。だれがどのようにして COBIT に到達するかが問題ではなく，以上の3種類の利用者のコンセンサスにより COBIT が採用されていれば，最大の効果を得ることができる。

一般的な組織では，組織内に COBIT を正式に採用するよう主張する人やグループ，すなわち COBIT 推進者が存在するだろう。COBIT を採用するコンセンサスを得るために，COBIT 推進者は誰に影響を及ぼす必要があるか，そしてその影響を最も効果的に及ぼす方法を決定すべきである。最善の方法を決定するために，COBIT 推進者は組織方針の決定者を識別し，組織内の主要な関係や目標を理解する必要がある。克服すべき課題は COBIT の採用を組織の方向性に結び付けることであり，COBIT が戦略的観点から意味があるという状態を構築することである。この導入ガイドは，組織全体で COBIT を採用することについて COBIT 推進者を支援するために設計されている。

COBIT の採用のために，誰に影響を及ぼす必要があるか？

COBIT は第一に，組織の情報および関連する技術を管理するための枠組みである。したがって，マネジメント，特に IT 方針の決定者は組織内の関係者の中で，COBIT の採用に影響を及ぼす上で主要な役割を演じる。そのような方針決定者の例として，チーフエグゼクティブ（CEO），シニア IT エグゼクティブ

(CIO, IT 部門の副社長), IT 運営委員会があげられる。IT 資源が組織目標の達成に向けられていることを保証する役割を COBIT が果たすことに, このグループは非常に関心を示すべきである。

IT ユーザーは上級の IT 方針決定者より幾分視野が狭いかもしれない。IT ユーザーは一般的に, IT が自分たちの日常業務にどの程度貢献するかということに, より多くの関心がある。しかしながら, IT ユーザーはまた, IT 資源を上手に利用してそれが自分たちの目標達成に役立っていることを知ろうとする。このグループの中で最も影響を及ぼすべき人には, 執行役員 (COO), ビジネスプロセスオーナー, 第一線のマネージャが含まれる。

組織内の複数の機能が IT の評価に責任を負っている場合がある。第一に, 監査人は IT が安全で組織のニーズに合致しており, コントロールされた手段で運営されているという保証を独立した立場から与える。第二に, ユーザは自分たちが要求している IT 資源が獲得され適切に利用されているかを周期的にレビューする場合がある。最後に, IT 機能は自分たちが組織に効果的かつ効率的な IT 資源を提供しているかを判断するための自己評価を行うだろう。このグループの中で最も影響を及ぼすべき機能は監査, 監査委員会, ビジネスプロセスオーナー, IT 専門家および IT マネジメントである。

公式あるいは非公式に存在する組織上の関係は, COBIT 推進者が誰と同盟関係および包括的な導入アプローチを形成するかということに影響を与える。次の要因を考慮すべきであろう。

1. IT の規模と組織構造はどうか。巨大で中央集権型で階層が高い組織では, トップレベル主導による公式的な採用プロセスが要求されるだろう。よりフラットな組織では, 関係するすべての部門が達成すべきゴールに同意し, COBIT の導入を一緒になって進めていくというコンセンサスアプローチを採用することができるかもしれない。
2. 監査組織の規模と構造はどうか。大きな独立した IS 監査グループが存在する大きな監査組織の中で COBIT を導入することは, IS 監査機能の中で始め, その後 IT 類似機能にあるいは監査マネジメントにまで広がるかもしれない。このアプローチはコンセンサスの醸成をもたらすことができるだろう。
3. IT と IS 監査との間の関係, および監査とマネジメントとの間の関係はどうか。監査組織の哲学は何か。革新的なビジネスアドバイザーである監査主体は, COBIT の採用についてのコンセンサスを容易に得ることができるだろう。実際, ビジネスプロセス, IT 資源の管理, ビジネス目標の達成を強調する COBIT 枠組みは, すでに存在している革新的なマネジメント指向的な監査哲学に対して, 追加的なガイドラインを提供するだろう。準拠性に焦点を当てる監査主体や, 監査クライアントとの関係がそれほど緊密でない監査主体は, COBIT 枠組み採用の命令に頼る必要があるだろう。これらの命令はチーフエグゼクティブや監査委員会から下されるかもしれない。
4. IT はどの程度アウトソーシングされているか。第三者機関との関係はどのくらいうまく管理されているか。第三者機関との関係がよく管理されているかあるいは IT がほとんどアウトソーシングされていない場合には, 組織の中で意思決定が下されるため, COBIT の採用はより簡単であろう。そうでない場合には変化を生み出すために, 第三者機関との契約更改や外部監査 (米国における SAS7

0のような）の影響が必要であろう。

5. 組織はどの程度ビジネスプロセスをリエンジニアリングしたか。ビジネス・プロセス・リエンジニアリングに関して，組織で何が進行しているか。COBIT は変更すべきビジネスプロセスを検討するための，またビジネスプロセス改善のための価値あるインプットを提供することができる。組織内における情報技術や情報関連技術の利用の高まりに対して，COBIT の強調はビジネスプロセスの改善に非常に実用的な指針を提供することができる。

なぜ組織は COBIT を採用する必要があるか？

これらの主要な方針決定者の間でコンセンサスを得るために，何がセールスポイントとして利用できるか。

1. 組織が経験した高次元の特徴的な問題は，企業統治問題に注意を集中させている。その結果，マネジメントは有効な内部統制システムを維持するよう，増大するプレッシャーを経験している。法的要請，受託責任，契約上の要求，社会的圧力が存在する。IT が支援するビジネス目標が達成されるであろうかということについて，また IT リスクがすでに認識されており，リスクに曝された部分が管理されているかということについて，合理的な保証を提供するために COBIT を利用することができる。
2. マネジメントは組織の資源の管理について説明する義務がある。マネジメントは IT 投資が最適であることをどのようにして知るのであろうか。COBIT に基づいた IT の有効性のレビューが，その質問に答える助けとなるだろう。例えば，COBIT は複雑な技術を管理し，その技術の急速な陳腐化に対するための計画を立案する IT プロセスを推奨する。
3. 上記に加え，次の4つの要因はマネジメントが COBIT を取り入れる動機となるだろう。
   a) IT 資源をコントロールすることにより，IT サービスを提供するためのコスト総額が下落するだろう。
   b) IT 資源がリスクに曝されている状態に対して脆弱である，あるいは，ビジネス目標が達成されないだろうというマネジメントの恐れ，不信，疑いを COBIT は減少させる。
   c) COBIT を採用すれば，適用される規則，規制，契約上の義務に組織が準拠していることを保証する助けとなる。
   d) ISO9000 の認証を得るように，「すでに COBIT を導入した」組織は IT 運用が適切に管理されコントロールされていることを明示することにより，競争相手との差別化を図ることができるかもしれない。
4. COSO（「部統制の統合的枠組み」）をすでに採用したか，あるいはほとんど採用している組織は，COBIT を同時に採用する機会がある。いくつかの組織からの報告によると，COSO と COBIT の同時導入は非常に円滑に行われたようである。というのも，この2つの枠組みは非常に相互補完的であるからである。つまり，COSO は関連するすべての内部統制を扱っており，COBIT はこれらのうち，特に IT に関する部分を扱っているからである。（同様のことはカナダの CoCo，イギリスの Cadbury，南アフリカの King の導入にも当てはまる。）
5. COBIT 枠組みの権威ある性質は，多くの組織が COBIT を採用することにより証明されてきた。

302 個のコントロール目標は 36 個の IT セキュリティ，監査とコントロール標準および世界的なベストプラクティス資源から開発された。

6. いくつかの組織においては，COBIT が解決できるような問題をかかえていた。例えば，ある組織では自分たちの IT 解決策がビジネスニーズに合致していないと判断した。彼らは適切なプロジェクト管理のプロセスを持っていたが，適切なシステム開発ライフサイクルプロセスを持ち合わせていなかった。彼らはこのようなプロセスの導入指針として COBIT を利用した。
7. すでに COBIT を採用した多くの組織の人々は，マネジメントとユーザと監査人との間のコミュニケーションが改善されたという経験を報告してきた。COBIT を利用して作成された監査計画書および監査報告書は，マネジメント用語（例えば，プロセス指向，トータル・クオリティ・マネジメント）で書かれており，マネジメントに関する問題（例えば，アカウンタビリティ，ビジネス目標の達成）に言及している。
8. 組織がダウンサイズするにつれ，管理とコントロールの資源がより制限されるようになる。COBIT は IT 関連のリスクに曝されている状態を識別し管理するリスク評価のための枠組みを提供する。
9. いくつかの内部監査の組織と外部の会計事務所は，COBIT を使うことにより，統合された監査を改善したと報告している。IS 監査人と非 IS 監査人は，自分たちの監査目標を調整し監査の発見事項を報告するために，COBIT を利用している。

要するに，マネジメントは IT のビジネス目標に対する貢献の合理的な保証を望んでおり，また IT 運用が満足のいくものであり，それがその置かれた環境における動向に適時に適合し続けていることを判断するためのベンチマークを求めている。COBIT はそのような保証を提供するために利用できる。

COBIT の範囲と制限は何か

成功裡に導入するために，COBIT とは何か，COBIT は何に適用できるか，COBIT は何をすることができるか，何が COBIT ではないのか，COBIT ができないことは何かということを，各自が明確に理解しておかなくてはならない。次のいくつかのポイントが当てはまる。

1. COBIT はひとつの考え方，新しい考え方である。採用が成功するためにはオリエンテーション，教育，研修が必要である。このプロセスに 40 時間以上の時間を割いたと報告する監査人もいる。
2. COBIT は当該組織向けに仕立て上げられるべき枠組みである。例えば，COBIT の IT プロセスはその組織に存在しているプロセスと比較されるべきであり，組織のリスクはレビューされるべきであり，IT プロセスのための責任は確立されるべきである。
3. コントロールと監査の参考資料として，COBIT は次のような資源といっしょに利用されるべきである。米国公認会計士協会(AICPA)や連邦金融協会検査評議会(EFIEC)が発行している監査ガイドのような産業別監査ガイド，情報システムコントロール協会の「コンピュータ情報システム(CIS)監査マニュアル」，内部監査人協会の「システムの監査可能性とコントロール（SAC）」のようなコントロールと監査の汎用的なガイド，特定のプラットフォームのガイド（例えば，IBM や Sun などのハードウェア用ガイド，Novell, VMS，トップシークレットなどのソフトウェア用ガイド）
4. COBIT は単に IT コントロールと監査手続書を集めたものではない。さらに重要なことに，COBIT

は一般的に多くの組織が扱われなければならない IT コントロール目標や，それらの IT コントロール目標に対するパフォーマンスの評価に使われる監査ガイドラインを含んでいる。COBIT は高次元の IT コントロール目標の識別と理解であり，それは内部統制の枠組みとして，またその IT コントロール目標に合致する適切な内部統制を選択し導入し実行するために奉仕する。COBIT はまた，IT コントロール目標の達成を阻害する恐れのある優先づけされたリスクを，ユーザが考慮することを間接的に可能にする。COBIT は多くの組織に密接に関連する IT コントロール目標の上に作り上げられたので，COBIT を利用することは効率的な評価を確実に行う助けとなる。なぜなら，単にコントロール「チェックリスト」方式を利用するアプローチは一般に，不要なコントロールや特定のリスクの抑制に役に立たないコントロールを組織に付け加えてしまうことに帰着するからであり，このことは経験的に明らかである。したがって，COBIT は，第一に IT コントロール目標，第二に関連する重要な IT リスク，第三に関連する効果的な IT コントロールの上に構築された評価ツールを利用することに意味がある。

5. 次の「あなたの組織へ COBIT を導入する方法」の節で述べられているように，成功裡に導入するために，COBIT 推進者はキーとなる人物を識別し，彼らを COBIT のよき理解者にし，COBIT の教育を施し，将来 COBIT を利用する人々を研修すべきである。

COBIT:多くの利用者のための成果物

例1は，なぜ，そしてどのようにして COBIT が多様な利用者によって効果的に利用されるかを示している。

COBIT マネジメント理解度診断ツール

この導入ガイドはいかなる組織においても，COBIT の「販売」，利用，導入の助けとなる。しかし，もっともやり遂げなければならないことの一つは，トップマネジメントの関心を引くことだろう。したがって，ガイドにはマネジメントの関心を引き，マネジメントの理解を高めるために，基礎的で有益なツールが2つ付属している。

- IT 統治自己評価書
- マネジメントの IT 関心度診断書

これらのツールは，組織の IT コントロール環境と IT コントロール問題の分析，理解，伝達の助けとなる。

IT 統治自己評価書

この簡単な IT 統治自己評価チェックリストは付録 1 として提供されており， COBIT プロセスのそれぞれについて，マネジメントに次のような質問が用意されている。

- プロセスはマネジメントのビジネス目標にとってどの程度重要か。
- プロセスはうまく実行されているか否か（重要性とパフォーマンスの組合せはリスクの十分な指標を提供する）。

- だれがプロセスを実行し，だれがプロセスの報告義務を負っているか（そして，報告義務は明確であり承認されているか）。
- プロセスとそのコントロールは公式化されているか否か。すなわち，アウトソーシングした活動に対して十分な契約書があるか，あるいは内部プロセスに対して明確な一連の文書化された手続があるか。
- プロセスは監査されているか否か。

マネジメントの理解度はリスク指標，公式化の程度，責任と報告義務の明確化の連係により強化される。なお，「わからない」という回答は，リスクの高さを示す強いメッセージである。
<付録１ － IT 統治自己評価書を参照>

マネジメントの IT 関心度診断書

第二のツールである，マネジメントの IT 関心度診断書はもう一つの強力な管理ツールである。というのも，それが，IT に関する最近の特定のマネジメント関心事（例えば，相互接続性，クライアント／サーバー，グループウェアなど）の多くを明らかにするからであり，IT プロセスは生じた関心事に対応するコントロール下にあることが重要である。

どのような特別な組織においても，多くの要因が COBIT「コントロール目標」の中の個々のコントロールの重要性に影響するだろう。これらの要因には，特にビジネス環境と IT 環境のあるタイプに関連するリスク，最近のコントロール機能がどの程度良いか，および効率性の向上や全体的なコストの削減が望まれる分野がある。ある組織に含まれる既知のリスク状況や優先度の高い問題を COBIT の一連のコントロール目標と対応させることによって，特に関連する事項を明確にすることが可能である。

キーワード	マネジメントの IT 関心事

キーワード	マネジメントの IT 関心事

管理	
提携	IT 主導戦略
統治	IT 方針と企業統治
競争	競争優位のための IT 利用
統合	IT インフラの統合
所有コスト	IT 所有コストの引下げ
要求されるスキル	スキルの獲得と開発

クライアント・サーバー・アーキテクチュア	
調整	要求の調整の失敗
アクセス・コントロール	アクセス・コントロール問題
互換性	技術インフラとの非互換性
エンドユーザ管理	エンドユーザ管理問題
バージョン管理	ソフトウェアのバージョン管理
所有コスト	高価な所有コスト

インターネット/イントラネット	
ネットワーク・アクセス	企業ネットワークへの無権限アクセス
機密メッセージ	機密メッセージへの無権限アクセス
トランザクション・インテグリティ	企業トランザクションのインテグリティの欠如

ワークグループとグループウェア	
品質管理	品質管理
アクセス・コントロール	アクセス・コントロール
手続	非公式な手続

機密データ	機密データの漏洩
可用性	サービス可用性の中断
ウィルス	ウィルスの感染

データ･インテグリティ	データ･インテグリティ
構成管理	構成管理

エンタープライズ･パッケージによる解決	
ユーザー･ニーズ	ユーザ要件の満足の失敗
統合	統合の失敗
互換性	技術インフラとの非互換性
サポート	ベンダーサポート問題
コスト/複雑性	高価/複雑な導入

ネットワーク管理	
可用性	可用性
セキュリティ	セキュリティ
構成管理	構成管理
付帯管理	付帯管理
コスト	コスト
サポート/メインテナンス	サポート/メインテナンス

付録 1 に示されている，マネジメントの IT 関心度診断書のマトリックスは，ガートナーグループが 1997 年に IT についてのマネジメントの関心事を調査した結果を利用したものである。ISACA によって一連のリスクとして開発された事項は，COBIT の 34 個の上位のコントロール目標としてすでに割当てられており，また関連するコントロールが一目瞭然に示されている。この技法を使うことによって，COBIT はある組織に焦点を当てることができ，またビジネスリスクの論点の背景を調整してコントロールの優先順位に焦点を当てることができる。

<付録 1　－ マネジメントの IT 関心事を参照>

例 1

あなたの立場	あなたのために COBIT が役立つ目標	あなたにとって有益ないくつかの特定のアプローチ
エグゼクティブ・マネジャー	企業内のすべての部門のために一般的な IT 統治モデルとして COBIT を受け入れ促進すること	IT に特別な事項に対して既存の内部統制枠組み (COSO のような) を補足するために COBIT を利用すること 明確な責任を割当てることと同様，ビジネスと IT との間の共通言語を確立するために COBIT プロセスモデルを利用すること
ビジネス・マネジャー	ビジネスに対する IT の貢献を管理し監視するような共通の全社的なコントロールモデルを確立するために COBIT を利用すること	ビジネス機能内で大規模にITを扱うことに対するよい実務の規約として COBIT コントロール目標を利用すること IT 機能 (社内，社外にかかわらず) と合意されたサービスレベル同意書 (SLA) によりカバーされる必要がある様々な局面を決めるために，COBIT コントロール目標を利用すること
IT マネージャー	IT サービス機能を，管理可能でコントロール可能でビジネス上の貢献に焦点を当てたプロセスに構成するために，COBIT プロセスモデルと詳細コントロール目標を利用すること。後者は品質，セキュリティ，有効性のドメインである。	サービスレベル同意書を確立しビジネス機能との意思疎通を図るために，COBIT コントロールモデルを利用すること プロセス関連のパフォーマンス測定のための基礎として COBIT コントロールモデルを利用すること IT 関連の方針と規範のための基礎として COBIT コントロールモデルを利用すること (SAS70 のような) 外部証明書と同様に，一般に認められたコントロール目標の適切な水準を確立するための基礎モデルとして COBIT を利用すること
プロジェクト・マネージャー	最小のプロジェクトと品質保証標準のための一般的な枠組みとして	一般に認められたフェーズを IT 計画立案，取得と開発，サービスの提供，プロジェクトの管理と評価の中に統合することをプロジェクト計画が保証するために COBIT を利用すること
開発者	開発プロセスに適用するためのコントロールに対する最小限のガイドとして，また構築されている情報システムに統合するための内部統制に対する最小限のガイドとして	開発プロジェクトにおいて適用可能な IT コントロール目標のすべてが取扱われていることを保証するために COBIT を利用すること
運用担当者	クライアントの目標に明確に焦点を当てたサービスの提供とプロセスの支援に統合された最小限のコントロールのための一般的な枠組みとして	運用方針と手続が十分に包括的であることを保証するために COBIT を利用すること
ユーザ	十分な運用上のあるいは開発下の情報システムに統合され	COBIT をサービスレベル同意書のガイドとして利用すること

あなたの立場	あなたのために COBIT が役立つ目標	あなたにとって有益ないくつかの特定のアプローチ
	た内部統制のための最小限のガイダンスとして	
情報セキュリティ担当役員	情報セキュリティを他のビジネス関連のIT目標に統合する方法を提供する，調和のとれた枠組みとして	COBIT を情報セキュリティプログラム，方針，手続を構築するために利用すること
監査人	IT 監査全体を決定するための基礎として，また IT コントロールの参考として	レビューと検証の規準として，また IT 関連の監査の枠組みを組み立てるために COBIT を利用すること

あなたの組織へ COBIT を導入する方法

重要人物への COBIT の紹介

そう，あなたは COBIT 推進者である。あなたは COBIT の採用を主張し，重要人物が誰かを識別し，あなたの組織内の公式また非公式の組織関係を理解する。今，あなたは COBIT 大使，つまり組織へ COBIT を導入する公式の担当者にならなければならない。COBIT が成功裡に採用されるには，オリエンテーション，教育および研修の各セッションを実施する必要がある。COBIT 大使が行うべき一般的なプロセスは，以下に記述のとおりである。(あなたが選んだ導入アプローチにそれを採用してもよい。)

上級マネジメントたちは，1 時間の「オリエンテーション」セッションを受けるべきである。短い ISACA スライド・プレゼンテーションを使用して － 次の問題点を強調する。

1. 内部統制システムの目的は，(i)「組織をその使命達成に向かうように維持し，途中の予期せざることを最小化すること」，および(ii)「急速に変化する経済環境および競争環境，顧客の要求や優先順位の変化，および未来の成長のためのリストラに対処すること」（ COSO「経営者のため要約」，1 頁 ）。コントロールの枠組みを全従業員が理解した上で採用する組織は，収益性，市場への浸透，顧客サービス，業界の主導権といった成功の尺度において，競争相手を凌駕することになる。
2. 内部統制は，広義には (COSO により)次のように定義される。「業務の効率性と有効性，財務報告の信頼性，および関連法規への準拠性といった範疇の目的を達成することに関して合理的な保証を提供することを意図した，事業体の取締役会，マネジメントおよび他の構成員によって遂行される一つのプロセス」(COSO「経営者のため要約」，1頁)。COSO は内部統制を，先ずは人々によって影響されるものであり，「目的に基づいた」 ものであると定義する。かくして，組織の全員がリスクコントロール評価の品質に責任がある。COSO はコントロールが全員の仕事であると考えている。
3. コントロールは，ビジネス目標を達成し，望まれない出来事を防止し発見する合理的な保証を与えるように意図された，方針，手続，慣行，組織構造であると(COBIT により)定義される(COBIT「枠組み」，11頁)。
   [これらの 3 点 (1 から 3) を要約すると，内部統制とは，途中で悪いことが起きるリスクを最小限にしながら，マネジメントが組織目標の達成の可能性を増やすプロセスである。COBIT および COSO は，IT および非 IT のそれぞれのコントロール上の問題に補完的に対処する枠組みである。(カナダの CoCo および UK の Cadbury にも同様の要約がある。)]
4. 技術がコントロールに与える影響を検討しなさい。すなわち，業務上およびコントロール上の目標がほとんど変わらないにもかかわらず(ある技術に特有のコントロール目標は変わるかもしれないが)，コントロール「手法」は技術革新によって最も直接的な影響を受ける。そして，COBIT が強調するコントロール「目標」は，技術革新に対応してコントロールを設計し導入し実行する責任がある人々にとって，ガイダンスとなる基礎的な枠組みを提供するであろう。
5. COBIT には技術関連のコントロール目標および手法が記述されており，それらは 36 個の国際的な一般に認められたセキュリティ，監査およびコントロールの参考資料から導き出されている。
   [これらの2点（4と5）を要約すると，IT のマネジメントとコントロールの標準として COBIT を採用

することにより，組織は IT 資源が組織目標を直接的に達成しているという合理的な保証を得ることができる。]

6. COBIT の内容をレビューして，オリエンテーション・セッションを終了しなさい。
   a. COBIT「枠組み」の中で， COBIT が情報規準，IT 資源，IT プロセスの間の関係をどのように文書化しているか記述しなさい。
   b. COBIT「コントロール目標」の中で，34 個の高次元のコントロール目標と 302 個の詳細コントロール目標との間の関係について記述しなさい。
   c. COBIT「監査ガイドライン」の中で，監査ガイドラインの性格および監査プロセスの構造をレビューしなさい。これらのガイドラインにより，IT プロセスを評価することができる。

残っている重要人物は，1〜2 日間の「教育」セッションを受けるべきである。長い ISACA スライド・プレゼンテーションを使用して，これらの導入ワークショップは彼らが COBIT 成果物のすべてを理解して利用し始めるのに役に立つであろう。(注：ISACA プロフェッショナル・セミナー・シリーズ[PSS] COBIT ワークショップには，スライド・プレゼンテーションを補う事例研究が含まれている。)次の順序はよく利用されている。1 人もしくはそれ以上の人が，各国でのあるいは国際的な ISACA ワークショップ(1 時間から 2 日間で)で COBIT の紹介を受ける。その後，組織の中でワークショップそのものを行うか，あるいは他のメンバーがワークショップに参加できるように手配する。これらのワークショップは，IS 監査人，他の監査人，マネジメント (一般，監査，IT)，ユーザおよび IT スタッフのためにも行われるであろう。

最後に， COBIT を実際に利用する人々は， COBIT を有効に使いこなすためにはより広範囲な「研修」を必要とするかもしれない。次の節 (COBIT を使い始める)で，COBIT を成功裡に導入する方法について述べている。この中で，COBIT の使い方に関しての実地訓練(OJT)を提供するために利用できる活動がある。

COBIT を使い始める

一旦あなたが自分の組織で COBIT を使うことに決めたら，正式に COBIT を使用するために，下記の事項を実施するかどうか検討しなさい。

1. COBIT が IT コントロールおよび監査にとって明確な方針と良い実務の例であるということを，組織の中で実施される監査の手引きとして使用されるであろう監査方針マニュアルの中で明記しなさい。
2. COBIT「監査ガイドライン」に含まれている「一般監査ガイドライン」を，監査手続マニュアルに含めなさい。
3. 以下の節 「COBIT を使用したリスク評価および監査計画」 で説明するように，リスク評価の実施と監査計画の策定の手引きとするために，COBIT「枠組み」を使用しなさい。
4. 以下の節「COBIT を使用した監査の実施」で説明するように，特定の監査契約を計画するために，COBIT「枠組み」および「コントロール目標」を使用しなさい。
5. 以下の節「COBIT を使用した監査の実施」で説明するように，COBIT 監査「ガイドライン」中の活

動を含むように監査手続書を作成しなさい。

次の活動，文書および考えは，COBIT の導入に成功した組織が使用した。これらのうちの多くは，どのような組織にも適切であろう。

例 2 は，銀行の IS 監査人が開発した導入実行計画である。プロセスに加えて，導入の目標およびゴールに注意しなさい。この計画は IS 監査人が立案したが，上位のマネジメントおよび他の重要人物を含む導入チームが，このような計画を立案しメモを作成するかもしれない。

完全な COBIT 導入を望まなかったりもしくはできなかったりして，慎重に選ばれた監査契約の中で COBIT の使用を開始した組織もあった。このような試験的導入は，COBIT 導入による効果を見極めるために行われた。すべての場合において，これらの試験的に導入した組織は結局，COBIT の完全な導入を行うことになった。例が最後の節「COBIT 監査ガイドライン」の中にある。

例2－COBIT 導入実行計画

目的

監査，業務および技術，アウトソーシングされるサービスを含む私たちの技術組織へ，COBIT 概念を取込み統合すること。

ゴール

1. 必須の監査およびコントロールのコンサルティングサービスを提供し続けて，銀行業界に関連する COBIT 業務プロセスのカバー率を保証するために拡張し適用すること
2. 銀行の情報ニーズは，COBIT が識別した情報規準と首尾一貫している私たちの技術組織により満たされていることを保証すること
3. COBIT が識別した重要な計画および組織活動が銀行の技術組織へ統合されていることを保証すること
4. COBIT が識別した重要な取得および導入活動がコンピュータ･サービス部門で採用され，銀行で使われるプロジェクト管理アプローチに取り入れられていることを保証すること
5. COBIT が識別した重要なサービス提供および支援活動がネットワークサービス部門およびアウトソーシング･サービス･ベンダーによって，銀行内部の顧客に提供されていることを保証すること
6. COBIT が識別した重要な監視プロセスが銀行の技術組織および監査組織によって採用されていることを保証すること

アプローチ

･広く知らしめること　･約束すること　･導入すること
･教育すること　･改良すること

順序

･監査組織　･アウトソーシング･サービス提供者　･監査委員会
･技術組織　･上級マネジメント

プロセス

1. 現行組織についての分析や考えを呼び起こすために，COBIT「経営者のため要約」および予備調査(例 3 参照) のコピーを主要なマネージャへ配布しなさい。
2. 調査結果を調製して，結果を COBIT 概念と関係づけるプレゼンテーションを作成しなさい。
3. 業務および技術のマネジメントへ提出しなさい。
4. 業務および技術のスタッフへ提出しなさい。
5. アウトソーシング･サービス提供者のマネジメントおよび主要なスタッフへ提出しなさい。
6. COBIT 概念を銀行の業務プロセスに組込むための実行計画を，主要なマネージャが作成するのを手助けしなさい。
7. COBIT 概念および活動進捗報告を上級マネジメントに提出して，内容を知らせ約束を取り付けなさい。

8. COBIT プロセスのオリエンテーションに反映するために，監査の成果物を再構築しなさい。
9. COBIT 監査ガイドと首尾一貫した監査手続書を作成または更新しなさい。
10. 組織のニーズと首尾一貫した COBIT 教育の機会を提供しなさい。
11. 必要な場合には COBIT 研修を実施しなさい。
12. IT実行計画の進捗を監視しなさい。
13. COBIT 概念，進捗，結果を監査委員会に提出しなさい。

マイルストーン

1. 5 月 - 調査および実行計画を完成する
2. 7 月 - 上級マネジメントへ COBIT を提出する
3. 8 月 - 監査委員会へ COBIT を提出する

COBIT を使用したリスク評価および監査計画

監査チームが予備監査の作業で次の COBIT ベースのマトリックスを使用すれば，監査あるいはマネジメント・アドバイザリー・サービス業務の潜在的な分野を識別することができる。マトリックスのいくつかは，監査を受けるマネジメントやビジネスプロセスオーナーに完成してもらうことにより，効果的に利用することができる。したがって，監査チームが監査を受ける側と共同でその様式を完成させることにすれば，予備監査でのインタビューやディスカッションが容易になるかもしれない。組織のコントロールまたは業務基準と関連付けられるべきであるが必ずしも遵守されていない業務分野で，しかもIT機能を実施する業務分野を早期に識別することにより，このディスカッションのいくつかは契約の開始時点においてマネジメントに大いに役立つかもしれない。それはまた，マネジメントがITの全プロセスに対して責任を負うポイントが明白であるということを保証すること，およびマネジメントが監査チームが誰とインタビューする必要があるか，あるいは誰から情報を得る必要があるかを識別することを支援する。これらのマトリックスは，監査人が内部統制についての文書を高次元で評価することを支援するかもしれない。監査チームは，内部統制についての文書がマネジメントによってレビューされ承認されたか否かを確認すべきである。ITプロセスについて文書化されたコントロールが存在しないことは，コントロールの弱点を示す危険信号として，またマネジメント・アドバイザリー・サービスの機会として考慮されるべきである。

過去の監査業務フォーム

目的: ITプロセスに関する監査業務が過去の監査範囲に含められていたか否かを識別すること。もし含められていたならば，監査人は過去の監査業務から導き出された結論を識別するために当フォームを求める必要がある。このフォームが完成していれば，これまでの契約において COBIT が使用されていると推定される。

作成者: 監査対象側と共に現場に訪問する前に予備監査業務を実施している監査チーム。

ディスカッション: もし過去の監査業務の実施結果が適正意見に相当するものであれば，それは解決が必要な監査発見事項はなかったということだろう。また個々のITプロセスに複数の発見事項があれば，監査人は発見事項の数を識別しそれらの処理を特徴付けるために，当フォームを求める必要である。もし1つのプロセスに複数の発見事項があれば，監査人は当フォームの処理欄に評価結果を数値で記載する。

<例２ － 過去の監査業務フォームを参照>

事業体短文フォーム

目的：どのITプロセスが最も重要だと考えられているか，またこれらのプロセスは実施されているということを，マネジメントがどの程度確信しているかについて識別すること。

作成者:

1.a. 監査プロセスのうち予備監査段階にある，監査を受けるマネジメント(IT部門担当，非IT部門担当)，あるいはビジネスプロセスオーナー。さまざまな部門から代表的なサンプルとして選ばれたマネージャに当マトリックスを提供すれば，それぞれのITプロセスの相対的な重要性やその効果のレベルを理解する上での違いを識別するために当マトリックスが利用されるかもしれない。

b. もしあるITプロセスが外部委託されていれば，マネジメントあるいはビジネスプロセスオーナーが外部業者の提供するサービスに対してどの程度満足しているかを判断するために，当マトリックスを利用することができる。そして，さまざまな部門から代表的なサンプルとして選ばれたマネージャがそのフォームを再度完成させたときに，提供されているサービスに対するさまざまな洞察が得られるかもしれない。

2. 個々のITプロセスの相対的な重要性と効果を理解して記録するために予備監査を実施する監査チーム。後者は，ユーザ満足度の調査を通じて得られた判断であるかもしれないし，マネジメントの業績評価から得られた結果に基づいたものであるかもしれない。(マネジメントが正式に業績を評価するためのプロセスがあるか否かを示すために，「正式な評価」欄には，「はい」なら「Y」，「いいえ」なら「N」を記入する。)

ディスカッション: 当フォームをマネジメントやビジネスプロセスオーナーに送付しなさい。送付する場合は，COBIT「枠組み」の中で見出されるITプロセスの記述を，このフォームに添付すべきである。(監査がインタビューを通じて最初に情報を入手する場合には，「事業体長文フォーム」を利用すべきである。)

「私たちにとって何が重要か」「私たちはどのようにすべきか」といった疑問に答えるために，このマトリックスを利用してリスク評価を行うことができる。これがマネジメント，監査人，IT部門の間のディスカッションに利用された事例がある。あるいは，これらのグループから別々に情報を収集するために，また結果を比較して重要性や効果についてどの辺に意見の合わない点があるかを判断するために，このマトリックスが使われるかもしれない。どのようなケースであっても，このマトリックスは非常に有用なディスカッションを実施するための触媒となり得る。例えば，あるグループが重要性のレベルを決定することができない場合は，何らかの教育の必要性が示されるかもしれない。あるいは，プロセスの業績が評価できない場合は，追加調査が必要となるかもしれない。

このマトリックスはまた，何度も繰り返し利用することができる。まず，業績の知覚レベルを決めるために，重要性欄のみを使用するだろう。しばらく経ってから(おそらく1週間)，再びそのマトリックスを業績欄のみ利用する。というのは，重要な機能が十分に実施されていないと評価することは困難であるかもしれないので，この2ステップのプロセスは，より有用な業績評価をもたらすであろう。

<付録2 － 事業体短文フォームを参照>

事業体長文フォーム

目的: どのITプロセスが最も重要であるか，そしてこれらのプロセスの運用が実施されていることをどの程度確信しているかについての，マネジメントおよびビジネスプロセスオーナーの評価を文書化すること。このフォームはまた，ITプロセスに対する内部統制について文書化した参考資料でもある。

作成者: 監査プロセスの予備監査段階にある監査チーム。監査人の一連のインタビューを通じてマネジメントおよびビジネスプロセスオーナーと共同して，あるいは監査チーム自身によってのいずれかにより，マトリックスを完成させるべきである。

ディスカッション:ITプロセスに対して内部統制がどの程度文書化されているかについてのマネジメントの理解について，監査人は洞察することができる。監査チームは予備監査を通じて，コントロールについて記述された文書のコピーを要求してきているので，調書のリファレンスには，コントロールについての文書(コントロールマニュアル，手続，基準等) のコピーとのクロスリファレンスを明示すべきであるし，または予備レビューを実施すべきである。

<付録２ － 事業体長文フォームを参照>

リスク評価フォーム

目的:リスクベース監査の実施が監査業務(あるいはマネジメント･アドバイザリー･サービス業務)を保証するというITプロセスを，監査チームが識別するのを支援すること。

実施者:予備監査業務を通じて，監査チームまたはマネジメントのどちらか一方，または両者の共同。

ディスカッション: 「事業体短文フォーム」と「事業体長文フォーム」を完成させ，その組織の使命，主要なビジネス目標，主要成功要因，規制や法律(契約を含む)の要求およびコントロール構造について十分に理解し記録した後に，監査チームはこのフォームを完成させる。監査チームは，この時までに何らかの分析を実施したかもしれない。

<付録２ － リスク評価フォームを参照>

責任者フォーム

目的:個々のITプロセスを誰が実行しているのか，そして個々のプロセスに対する最終責任を誰が負っているのかを識別すること。

実施者:

監査の予備監査段階にある監査チームと監査対象企業のマネジメントとの共同。

マネージャとビジネスプロセスオーナーに当フォームを送付する場合は，COBIT「枠組み」の中で見出されるITプロセスの記述を，このフォームに添付すべきである。例として，例3「COBIT 調査」を参照のこと。

ディスカッション：ITサービス部門が，あるいはITサービス部門だけでなく外部業者が事業体に提供しているサービスを十分に識別するために，契約サービス/サービスレベル協定(SLA)フォーム(次節で議論される)と一緒にこのフォームを完成させることを提案する。

ITに普及しやすい性質があるとすれば，複数のプロセスがITサービスと非ITサービス双方の担当者によって実行されることもあり得る。その点で，上席のマネジメントと共同でフォームを完成させることは，どのプロセスが誰によって実行されているかについてのマネジメントの理解に対する洞察を得ることにもなる。それはITに普及しやすい性質がある組織であるなら，組織横断的にIT責任が広がることをも強調するだろう。

ITプロセスおよびそのプロセスが取扱っているものが多少当たり前であっても，それぞれのプロセスによってカバーされていることの概要をマネジメントに提供するために監査チームが作成することが望ましい。また，内部であれ外部委託であれ，どの機能単位がITプロセスを実行しているかということを，マネージャがどこまで明確に理解しているかを識別するために，組織横断的に異なる部門のマネージャをインタビューしている時にも，そのフォームは利用されるかもしれない。

当フォームは監査チームに誰が主たる責任を持つのかを識別することを求めるが，それは割当てられた責任，報告責任の要点，分散したまたは「広がった」ITプロセス活動に関する予備監査でのディスカッションのための開始点として，考慮されるべきである。後者の例として，決められた組織の中で，業務処理がITサービス部門から個々の部門にシフトしたとしても，それはITサービスに関するデータセキュリティやシステム可用性のコントロール目標がもはや適合しないということを意味するものではない。コントロール目標は，今や異なる組織単位ごとに，そして一般に異なるコントロール戦略をもって提示されていなくてはならない。

<付録２ － 責任者フォームを参照>

契約サービス/サービスレベル協定（ＳＬＡ）フォーム

目的:「責任者」マトリックスが，１つあるいは複数のITサービスがITサービス部門によって実行されていないことを示しているならば，正式な契約やサービスレベル協定が存在するか否か，また，コントロールが「契約した」ITプロセスごとに文書化されているか否かを，このフォームは識別する。契約/サービスレベル協定を結んだITプロセスは次の内容を含む。外部委託したサービス，内部契約のサービス

(組織内，ITサービス部門に限らない)，そして内部のサービスレベル協定が存在するサービス。そのフォームは，明白な契約や協定なしで「契約状態」であった機能を，監査人が識別するのを支援するかもしれない。それゆえにそのフォームは，監査範囲内で契約/サービスレベル協定の監査業務に対する潜在的なニーズを識別することを支援するだろう。

実施者：監査の予備監査段階にある監査チーム。

ディスカッション：契約サービス/サービスレベル協定フォームは，監査人の内部統制評価を支援する。確立されたコントロールの適正性を評価する前に，監査人はどの範囲のコントロールまで文書化されているかを判断するであろう。

<付録 2 － 契約サービス/ SLA フォームを参照>

計画立案マトリックスの使用例

COBIT 導入の開始時に，最初の評価として，IS監査人は銀行の調査を実施した。その調査は例 3 として添付されているが，「責任者フォーム」の適用である。調査は業務担当，技術担当の上席副社長に直接に報告する人々に対して実施された。その調査に添付された 4 ページの資料は，COBIT パッケージに含まれるテキスト･ファイルを使ってIS監査人が開発したデータベースから印刷された。調査の結果，全員が COBIT プロセスの大部分に責任を負っていることが判明した！ IS監査人は，副社長からの明確な指示の欠如が，割当てられた責任が明確でないことの原因であると結論づけた。この調査および規制監査の発見事項の結果として，技術管理機能が業務担当，技術担当の組織に加えられた。この機能は，COBIT の計画立案と組織化プロセスの多くに対する責任を割当てられた。

例3－COBIT 調査

メモ

宛先: ネットワーク・サービス・マネジャー，テレコミュニケーション・マネジャー，プログラミング・スーパーバイザー，計算センター運営マネージャ，共同計算センター・マネージャ

写し: 業務担当上級副社長，技術担当上級副社長，外部委託アカウント・マネジャー

差出人: IS監査マネージャ

日付: 19 xx 年 3 月 19 日

件名: 情報サービスビジネスプロセスとコントロール目標

IT分野における内部統制に関する新しい観点を皆さんに紹介したいと考えています。そして，私たちがより革新的なより支援的な監査人になるために，皆さんの支援をお願いしたいと考えています。コントロールやITに対する従来の監査アプローチは，技術的な問題を強調する傾向にありました。情報システムコントロール財団(ISACF)は最近，情報規準とビジネスプロセスに焦点をあてた新しいコントロール目標に関する文書を発表しました。

IS監査の世界で過去 20 年間用いられてきたガイドラインで，情報システム，アプリケーションおよび運用におけるコントロールの妥当性を評価するためのガイドラインを，ISACF が改訂しました。この新しいガイドラインは，「情報および関連技術のためのコントロール目標」または COBIT と呼ばれ，それは 34 個の重要なITビジネスプロセスを，計画立案と組織化(PO)，取得と導入(AI)，サービス提供と支援(DS)，監視(M)の 4 つのドメインの中に識別します。さらに COBIT は，302 個の異なるタスクと活動をこれら 34 個のプロセスに関連付けています。これらのタスク，活動およびプロセスのそれぞれには，監査活動上焦点を当てることのできる，関連するコントロール要素があります。

したがって，COBIT はIS監査にとって，ITビジネスプロセスに対する私たちの監査を再構築するための大きな機会を提供します。COBIT はまた，必要なサービスをすべて銀行に提供しているということを保証するために，情報サービス部門が自己評価する機会を提供します。皆さんのレビューのために(まだ見ていない人のために)，COBIT の経営者のため要約のコピーを添付しました。

監査機能の再構築を始めるために，皆さんがこれらのITビジネスプロセスに対する自分の所有権や責任をどのように見ているかを知りたいと考えています。34 個のプロセスすべてを列挙し，そのプロセスに対する責任を持っているか否かの回答を求める事前調査を，私はこのメモに含めました。3 月 28 日までに，皆さんの回答および COBIT に対する皆さんの考えが得られれば，幸いです。私はオーバーラップする部分とギャップのある部分が見つかることを期待します。そして，この調査の目的が今日の私たちの状況を発展することであるということを覚えていて下さい。情報サービス部門における自分たちの役割を他の者がどのように見ているかを皆さんそれぞれが理解できるよう，調査結果を提供するつもりです。

私はこの変化にははっきり言って興奮しています。というのも，皆さんがビジネスの情報サービス分野を

運営する方法に沿って私たちがIS監査活動を行うことを，この変化は手助けするからです。私たちは，「プロダクト」監査に加えて「プロセス」監査を実施することができるのです。私たちは，継続的なプロセス改善に専念することができるのです。秘匿性，一貫性，可用性，効率性，有効性，準拠性および信頼性といった，情報と技術のリスクと規準に対する監査に取り組むことが，より容易になります。それはまた，私たちのデータ，アプリケーションシステム，技術，人々および設備といった資源にコントロールを関係づけることができます。要するに，私たちがツールや手引きとして COBIT を利用すれば，監査は皆さんにとってよりよい資源になり得るのです。

もし，この調査の対象となるべきであると皆さんが思われるマネジメントスタッフが他にいれば，あるいはこの調査や COBIT 概念全般について質問や意見があれば，外線 xx または E メールで私宛連絡して下さい。調査結果は 3 月 28 日までに社内便で返送して下さい。以上。

例3続き

予備調査 – ITプロセスに対する責任:

分野: **日付:**
回答者: **監査人:**

ドメイン ID	プロセス ID	次の IT プロセスについて責任がありますか？	IT プロセスが達成すべきビジネス要件	(はい・いいえ・わかりません)
PO	1	戦略的な情報技術計画の定義	情報技術の機会と IT ビジネスの要求の最適バランスへの進行と将来の確実な遂行の保証	
	2	情報アーキテクチュアの定義	最適な情報システムの構築	
	3	技術的な方向性の決定	利用可能で急成長中の技術の優位性の獲得	
	4	組織と関係の定義	IT サービスの提供	
	5	投資管理	資金調達の保証と財務資源の支出管理	
	6	経営目的と方向性の伝達	経営目的に関するユーザの知識と理解の保証	
	7	人的資源の管理	IT プロセスへの人的貢献の最大化	
	8	外部からの要求への準拠の保証	法律, 規則および契約の遵守	
	9	リスクの事前評価	IT 目標の達成の保証と IT サービスの提供に対する脅威への対応	
	10	プロジェクト管理	優先順位の設定と計画どおりかつ予算内のサービス提供	
	11	品質管理	IT の顧客要求の満足	

注記とコメント:

ドメイン ID	プロセス ID	次の IT プロセスについて責任がありますか？	IT プロセスが達成すべきビジネス要件	(はい・いいえ・わかりません)
AI	1	自動化された解決策の識別	ユーザの要求を満たす最良のアプローチの保証	
	2	アプリケーションソフトウェアの取得と維持	ビジネスプロセスを効率的に支援する自動化された機能の提供	
	3	技術インフラの取得と維持	ビジネスアプリケーションを支援するための適切なプラットフォームの提供	
	4	IT システム関連手続の開発と維持	採用されたアプリケーションおよび技術的な解決策の適切な利用の保証	
	5	システムの導入と信任	解決策が意図された目的に適合していることの検証と確認	
	6	変更管理	中断の可能性，未承認変更およびエラーの最小化	

注記とコメント:

ドメイン ID	プロセス ID	次の IT プロセスについて責任がありますか？	左の IT プロセスが達成すべきビジネス要件	(はい･いいえ･わかりません)
DS	1	サービスレベルの定義	要求されるサービスレベルの一般的な理解の確立	
	2	第三者サービス機関との関係の管理	第三者機関の役割と責任の明確な定義と忠実な実行および要求事項に対する継続的な満足の保証	
	3	パフォーマンスとキャパシティの管理	適切なキャパシティの利用可能性の保証と，要求されたパフォーマンスニーズを満たすための最良かつ最適な利用の保証	
	4	継続サービスの保証	要求されたサービスの利用可能性の確保と中断したサービスの復旧	
	5	システム･セキュリティの保証	未承認の利用，開示，修正，損傷，紛失に対する情報の保護	
	6	コストの識別と帰属	IT サービスに帰属するコストの正しい理解の保証	
	7	ユーザの教育と研修	ユーザが技術を有効に利用し，存在するリスクと責任を認識することの保証	
	8	IT の顧客の支援と助言	ユーザが遭遇した問題の適切な解決の保証	
	9	構成管理	すべての IT 構成要素に対する責任の明確化，未承認変更の予防，物理的存在の検証，正しい更新管理の基礎の提供	
	10	問題や事故の管理	問題や事故の解決と再発を防ぐための原因調査の実施の保証	
	11	データ管理	入力，処理，出力の間，データが完全で正確で妥当であり続けることの保証	
	12	ファシリティー管理	人災あるいは自然災害に対して IT 設備と人間を保護する適切な物理的環境の提供	
	13	運用管理	重要な IT 支援機能が規則的に整然と実行されることの保証	

注記とコメント:

ドメイン ID	プロセス ID	次の IT プロセスについて責任がありますか？	左の IT プロセスが達成すべきビジネス要件	(はい・いいえ・わかりません)
M	1	プロセスの監視	IT プロセスに対して設定された目標の達成の保証	
	2	適切な内部統制の割当て	運用上のセキュリティと内部統制の有効な運用の保証	
	3	独立的保証の入手	特定の IT 活動に関するセキュリティ，内部統制，有効性，準拠性の信頼水準の向上	
	4	独立的監査の提供	IT 内部統制およびセキュリティ環境に関する経済性，効率性，有効性の信頼水準の向上とベストプラクティスを参考にした提案	

注記とコメント:

例 4 のマトリックスを利用することにより，ある組織のある IS 監査人は COBIT の 34 個の高次元のコントロール目標を自分の組織の IS 方針，手続，基準に当てはめた。これは，IS 監査人が文書化された方針を徐々に発見する度に繰り返されるプロセスであった。最初に量的な評価をした後，当該組織において，このプロセスは既存の方針，手続，基準の品質と妥当性の評価へと続いていく。これには「事業体長文フォーム」を適用し，文書化されたコントロールが表す既存の方針や手続へのクロスレファレンスを欄に記入していくことである。

例 4：方針，手続および基準のレビュー

COBIT の 34 個のプロセス	IT 方針と手続 A B C D E F - - -
P O 1 P O 2 ・ ・ ・ M 4	A＝COBIT 目標へのアドレス C＝望まれる目標の提供 E＝評価（準拠性のテスト） R＝報告　・積極的な結論 ・発見事項

別の組織では，IS 監査人は COBIT を使ってリスクを評価し，彼が注目すべき監査分野を選んだ。例 5 は，彼がこの評価のために使ったマトリックスを表している。この評価において，COBIT 情報規準と IT 資源が際立った役割を演じている点に注意する必要がある。このマトリックスは，「過去の監査業務」フォームと「リスク評価」フォームの要素を結合したものである。

例 5：リスク評価のための COBIT の使用

監査分野	要素：直前の監査日，情報規準，IT 資源，不満/要求，リスクに曝されている状態
	リスクのランク　－10～＋10 それぞれのプロセスの合計とそれぞれの監査分野の合計

別の組織において，当期における追加的な方針，手続または基準，あるいは追加的な監査上の留意事項を必要とする分野に IS 監査人と IT 専門家の注意を集中するために，例 6 で示されたマトリックスを使用すべく IS 監査人と IT 専門家が協力した。これには，「リスク評価」フォームを適用する。

例 6： リスク評価

COBIT の 34 個のプロセス	リスクの評価レベル			注記
	高位	中位	低位	
P O 1 P O 2 ・ ・ ・ M 4				

ある監査部門では，IS 監査人は自分たちの現在および計画中の監査適用範囲を評価するために，COBIT の 34

個のプロセスを使っている(例 7 参照)。彼らは，IT プロセスのどのような種類にどのくらいの監査負荷を費やせばよいか，またどの IT プロセスに問題があるか否か(すなわち，多くの監査上の指摘事項があるか)を知りたいと考えている。さらに，彼らは，どの事業体が監査を受けたかあるいは受けるだろうかということを，そしてどのような種類の監査が実施されたかあるいは実施されるだろうかを知りたいと考えている。

例 7: 監査計画

COBIT の34個のプロセス	監査 (または監査実体) ABCDEF ---
PO1 PO2 ・ ・ ・ M4	S＝予備監査調査 A＝監査 R＝報告　・積極的な結論 ・発見事項

要約すれば，これらのベンチマーク／評価／計画立案の諸活動のすべては，組織に次のような追加情報を与える。

- 追加的な(または文書化された)方針，手続または基準が要求される。
- IT プロセス (またはコントロール) は，追加または除去される必要がある。
- IT プロセスに対する責任者は任命または再任命される必要がある。
- 関心をはらうべきリスクがある。
- よりよく管理されるべき内部またはアウトソーシングされる機能がある。
- 実施されるべき監査がある。

COBIT を使用した監査の実施

次に，上述のさまざまな COBIT の局面，およびリスク評価マトリックスと計画立案マトリックスが「典型的な」監査業務においてどのように使われるのか，その概要を記述する。

1. **任意のステップ。**必要なら，監査を受ける事業体のために「監査契約の種類を選択する。」実施される監査の種類として次のものがある。財務，業績，準拠性，IT (設備，開発中のシステム，稼動後のレビュー，計画立案と組織化，マネジメント・アドバイザリー・サービス)，統合監査，合意した手続，等々。これらの監査は，相互に相容れないものではない。COBIT「枠組み」と，これまでに説明した「事業体短文フォーム」，「責任者」マトリックス，「契約サービス/SLA」マトリックスと類似するツールを使ったリスク評価が，監査契約の種類の選択を容易にする。
2. **範囲を吟味して監査目標を決定する。**事業体と監査契約の種類の選択が終われば，今が COBIT の詳細コントロール目標 (COBIT「コントロール目標」から) を利用して，当該監査のために選択された IT プロセス (COBIT「枠組み」から) に対する追加的な洞察を得る時である。一旦範囲が吟味されたら，COBIT「コントロール目標」を利用して監査目標を明らかにする。契約前の打合せにおいて，範囲と監査目標をクライアントとディスカッションする必要がある。注：このステップは，監査期間中，必要な都度繰り返されるかもしれない。
3. **監査手続書を作成する。**
   a. すでに監査手続書がある場合
      i. 監査目標を COBIT「コントロール目標」と対比する。
      ii. 監査手続書上のステップを COBIT「監査ガイドライン」における活動と対比する。
      iii. 特定のプラットフォーム(たとえば，セキュリティ・パッケージ，LAN)上，組織的上，法律上および規制上のガイドおよびマニュアルによって示唆される監査活動を追加する。
   b. 監査手続書がない場合
      上述のようなステップを実施するが，既存の手続書を COBIT と対比して完成するよりは，COBIT を使って新たに監査手続書を作成する。

4. **監査を実施する。**種類，範囲および目標について最初の協議を行い，COBIT がこれらにどのように貢献したか，また COBIT が監査を導くためにどのように使われるかということを説明する。
5. **監査報告書を作成する。**達成された目標および達成されなかった目標に焦点を合わせて結論を記載する。COBIT を使って，ビジネス事例を作成して結果に十分な根拠を与える。規準が監査上の指摘事項の中で引用される区分において，および監査を実施する際に使われた方法論について述べる区分において，COBIT について言及する。

COBIT ガイドラインの利用

上述のように COBIT ガイドラインの利用は，二つの主なカテゴリーに分類される。監査人が既存の監査プログラムを有しているか，有していないかである。

既存の監査プログラムがない場合

下図は，監査すべきITがあるが，監査プログラムが存在しない場合のステップを描写している。この例で示すITプロセスは，システム開発方法論（SDM）である。

ステップ＃1では，監査人はSDMを適用可能な COBIT の詳細コントロール目標（コントロール目標における）と比較して，SDMがシステム開発に対する適切なコントロールを提供するかどうかを判定する。

それが満足されたと仮定して，監査人はステップ＃2において，主題のITプロセス（SDM）のリスクと関連目標の理解のもとで，最も重要な詳細コントロール目標を選定する。COBIT は提供された情報の七つの品質が組織目標を達成するために取り扱われていることを保証するためのIT資源のコントロールに焦点を当てているので，監査人がこの判定を行うことを支援する。

ステップ＃3において，監査人は COBIT 監査ガイドラインの支援のもとで監査プログラムを開発する。我々は，関心のある詳細な目標定義しているが，COBIT監査ガイドラインは高いレベルのコントロール目標（つまり，ITプロセス）により，グループ化されていることことに留意すること。

ステップ＃4において，監査人は監査プログラムのどのステップに最も注目すべきかを判定する。ステップ＃2で最も重要な詳細コントロール目標を選定して居るので，このステップは単純である。

ある組織では，変更コントロールの監査に COBIT を使用することで監査計画プロセスを促進し，監査とITによる COBIT のさらなる活用をもたらしている。Exhibit 8は，この変更コントロール監査プログラムからの抜粋である。“ビジネス目標”は，COBIT の枠組み（・レベルのコントロール目標）から適用されている。“影響”は，当該監査のために組織によって記述されたリスクである。“コントロール目標”は，COBIT のコントロール目標から適用した。“レビューテストすべき項目”は，COBIT 監査ガイドラインから適用した。これは，COBIT に基づいた監査プログラムの開発に典型的なものである。

a. COBIT の34の・レベルのコントロール目標をレビューし，当該監査に適用する　目標を選定する。

b. ステップaで選定したそれぞれの目標を達成することに失敗したことから生ずるリス　ク（または“イクスポジャー”または“影響”）を記述する。

c. 当該監査に適用する詳細なコントロール目標を COBIT コントロール目標から選定　する。通常，上記のステップaで選定した・レベルのコントロール目標に対する詳細なコントロール目標のみをレビューすれば良い。

d. COBIT 監査ガイドラインを使用して，実施すべき監査手続きを列挙する。このステップで，IS監査人は，上記のステップcで選択した詳細コントロール目標に関連　する監査手続きを選定すべきである。もし，ステップcにおいて，ステップaで識別　した・レベルのコントロール目標に対する詳細なコントロール目標のみを選定してい　たならば，その・レベルのコントロール目標に対する監査ガイドラインのみをレビュ　ーすれば良い。

e. 監査プログラムを完成するためには，IS監査人は監査対象の特定プラットフォーム　に関連する追加の監査テストを含む必要があるかもしれない。例えば，監査人はこの　システム開発作業に対して選択されたデータベース管理システムのマニュアルを参照　する必要があるかもしれない。

Exhibit8 監査プログラムからの抜粋

	ビジネス目標	影響	コントロール目標	レビューテストすべき項目	参照
A16	変更管理				
			変更コントロールの開始とコントロール		
	ユーザ要件を満たす全ての可能な代替案の分析を介して，自動化された解決法が識別されていることを保証する。		変更コントロール手続きに従えないと事故，データとファイルの破壊，処理の遅延，コストの増加とユーザとシステムの要件が満たされないことになる。緊急事態におけるリスクを増大する。マネジメントは，変更に対する全ての要求が正規の変更マネジメントプロセスに従っていることを保証すべきである。変更は分類され，優先位づけされ，また，緊急事態を取扱うために特定の手続きを作成すること。システム変更手続きについて，十分な内部統制があることなどをレビューする。エマージェンシィ時においても，システム変更手続きが有効であり，強制されていることをテストする。		
			変更のコントロール		
	構成管理システムとの不十分な統合は，他のプラットフォームに影響する。マネジメントはシステム変更管理ソフ				

トウェアのコントロールと配付が包括的な構成管理システムと適切に統合されていることを保証すべきである。包括的なマネジメントシステムへの順守を保証するために適切なドキュメンテーションをレビューし，テストする。

既存の監査プログラムがある場合

下図は，監査すべきITがあり，COBIT 監査ガイドラインに対するベンチマークを欲している監査プログラムが存在する場合のステップを描写している。繰り返すが，この例に使用されているITプロセスはシステム開発方法論である。

ステップ＃1，ステップ＃2とステップ＃4は，既存の監査プログラムがない場合と同様である。
ステップ＃3において，監査人は COBIT で示唆されている活動が既存の監査プログラムを改善するかどうかを判定するために，自身の監査プログラムを COBIT 監査ガイドラインと比較する。

COBIT の詳細コントロール目標を監査ガイドラインに対して位置づける。

上述のように，COBIT監査ガイドラインの活動は，34の･レベルのコントロール目標によりグループ化されている。監査人は通常，詳細なコントロール目標の達成を評価するために監査プログラムを開発する。例えば，監査人が一つの詳細なコントロール目標（確認すべき不合理な作業）。さらに，一つの目標がAI 1．17 技術の受容（コントロール目標参照）であるとする。下記の監査活動は，詳細なコントロール目標 AI 1．17に関連しているので，監査ガイドラインの監査活動から選択される。

理解

- 面接対象者：
  - ･プロジェクト所有者／スポンザー
  - ･契約者マネジメント

- 収集すべき証拠資料:
  - ･システム開発ライフサイクルとソフトウェアの購入に関する方針と手続
  - ･IT目標と長期および短期計画
  - ･選択したプロジェクトドキュメンテーション，要件定義，代替案分析，技術的可能性研 究，経済的可能性研究，情報フアーキテクチャー／企業のデータモデル分析，リスク分 析，内部統制／セキュリティのコスト効果研究，監査証跡分析，生物工学研究，設備と 特定技術の受容計画とテスト結果。
  - ･ソフトウェア購入，開発と保守に関する選択された契約。

コントロール評価

- 評価視点:
  - ･下記を要求する方針と手続
    - ･解決策のパフォーマンス，安全，信頼性，適合性，セキュリティと法規を含む充足すべき機能的と運用上の要件
    - ･製品は使用と財務的決済に先立ってレビューし，テストする。
    - ･完成した契約のプログラミングサービスの最終製品は，情報サービス機能の品質保証グループとその他の関連組織によって作業に対する支払いと最終製品の承認以前に関連する標準により，テストされ，レビューされる。
    - ･特定技術に対する検収計画は，契約により供給者と合意され，この計画は検収手続きと 基準を定義していること。
  - ･契約の仕様に含まれているテストは，システムテスト，統合テスト，ハードウェアと部 品のテスト，手続のテスト，負荷とストレスのテスト，チューニングとパフォーマンス のテスト，回帰テスト，ユーザの検収テスト，そして最後に予期しないシステム故障を 避けるための全体システムのパイロットテストが含まれる。

・特定の技術的検収テストは，検査，機能テストと負荷の試験を含むべきである。

► 準拠性テスト:

・購入製品は，使用と財務的決済に先立ってレビューし，テストする。
・検査，機能テストと負荷の試験を含む特定技術の研修計画の適切性と完全性

コントロール目標の不達成によるリスクの実証

►実証性テスト:

・同様の組織または適当な国際基準／認識されタイル産業の最善の慣行に対する自動化された解決法に合致するユーザ要件の識別のベンチマーキング
・検査，機能テストと負荷の試験が契約であきらかにした要件に合致していることを保証する特定技術に対する検収プロセスに対する詳細のレビュー。

► 実証性テストの結果:

・組織のシステム開発ライフサイクルの欠陥
・ユーザ要件を充足していない解決法
・組織で確立された購買アプローチに従っておらず，そこで，組織に対して追加コストを 生ずることになる解決法。
・特定記述が受け入れられたが，検査，機能テストと負荷の試験が適切に実施されておらず，その結果，技術がユーザ要件とまたは契約条項に従っていない。
・システムの故障

付録1 マネジメントの懸念の診断
IT統治(管理)の自己診断
マネジメントのITの関心事

付録2 ITのコントロールの診断
既往の監査作業の様式
実体の短文形式
実体の長文形式
リスク評価の様式
責任団体の様式
契約サービス／サービスレベルの合意(SLA)様式

COBIT のケーススタディ

マイケル　P　ラス，CISA，上級ITマネージャ，セデルグループ，ルクセンブルグ

要約

セデルグループがビジネスを行う方法の大きな変革は，コントロールと更新の方針記述をレビューする必要を生じた。成功する COBIT の導入は，上級マネジメント，ITSエンドユーザの間のチームとしての作業である。ビジネスの指導者はIT監査とコントロール活動から付加価値を得るので，ビジネス目標は，監査とコントロール方針と密接に結合している。

背景

66の世界の主要な金融機関から1977年，決済機関として設立されたセデルグループは，特に，成長しているユーロ債券市場，国境を越えた債券取引の決済のリスクを最小化した。ルクセンブルグ，ドバイ，香港，ロンドン，ニューヨークと東京に800人以上の従業員を抱え，30国以上の証券市場への結合を確立している。1997年の決済の総取引高は，15兆米ドルを越え，セデル銀行は1．4兆米ドルの顧客の株券を保管している。成長する国際ビジネスは，1，500億米ドルの一日平均の決済となっている。

我々の以前のIT環境は安定し，信頼でき，ビジネスの要件を満たしていたが，コントロールされた環境を維持するために変化が必要になった。1980年代の後半，我々は主要な新規ビジネス機会，高度なITの要求，新規のクライアント／サーバアプリケーションの開発，PCと通信ネットワーク環境の劇的な変化を経験した。

セデルグループのシステム方針ステートメントは，適用でき，実施されていたが，コントロール要件に規定された方法が新しい環境にはふさわしくない状況がますます発生してきた。例えば，以前のDOS／Novel環境に関連した方針は同時に二つ以上サインオンすることを防止するコントロールが存在していた。これは，現在，もしユーザが通常の職場でサインオフできないときに，コンテンジェンシィサイトからユーザがアクセスすることを防止していた。方針要件の放棄と変更要求が一般化してきた。

プロセス

大きな技術上，環境上とプロセスの変化に適用されたコントロール方針を開発し，維持する難題に直面して，我々はIT監査アプローチを検査する機会を使用した。幾つかの代替的方法論がレビューされたが，最も適切であるのが COBIT であることが判明した。 1996年，我々は枠組みを監査似て起用することで COBIT の実施を始めたが，その後，首尾よく実施された。

我々のIT部門は，監査結果により刺激され，独立にセデルグループのステートメントの新しいセットの枠組みとして COBIT を見なした。処理と通信の部長はそのレビューの議長であったが，“COBIT はそのコントロール目標を実用的である新しく，かつ，論理的方法で示している。”と述べている。セデル方針の完全な COBIT レビューの結果は，元気づけられるものであった。作成された新しい方針は全ての技術的プラットフォームに適用された。Plus 上級マネジメントは，よりリスクとコントロールを意識するようになった。ビジネス目標に合致し，かつコントロール要件を管理することの伝統的な葛藤は，マネージャがコントロールのビジネス上の利益をしばしば認識するようになったので，課題となることは少なくなった。

結論

我々が COBIT を導入するとき，実務的なビジネスと効率の優先度に新しく，かつ，強い焦点を当てることは，最も顕著な相違である。その原則に従って，我々は被監査部門自身のビジネスとオペレーション目標に基づいた監査を確立した。監査は今や中間から下方にアプローチするのではなく，トップからアプローチされている。COBIT の導入は，非常に効果的な監査方法であり，上級マネジメントは監査がビジネスに価値を付加していることが分かっていることを証明している。

我々の組織が COBIT 導入に成功したことに基づいて，それぞれのITマネジメントともに COBIT を調べるように同僚に勧めている。COBIT は，産業に関係している全ての人の利益になるコントロールされた環境を維持し，改善する非常に柔軟で信頼できるアプローチである。

ジョン　ベベリッジ，CISA
米国マサセーチューセッツ州監査人室

要約

州監査人室は，マサセーチューセッツ州政府の主要な政治監査実体である。我々は，監査選択において，個々の用務と実証結果に対して COBIT を幅広く使用している。IT監査部門は，６００以上の監査実体における２４の大規模データセンターと１５０以上の中小設備を含む複数のプラットフォーム環境で，統合した監査，財務関連監査，業務監査とIT監査を実施している。

プロセス

我々のIT監査管理チームは，フェーズアプローチを使用している。そこでは，IT監査スタッフのあるメンバーは，監査に活用するために，枠組み，コントロール目標と監査ガイドラインを導入した。チームが選択した監査は，IT設備の検査が範囲に含まれ，特定のアプリケーションシステムの開発中監査のシステムであった。

管理チームと選抜された上級監査人が他のスタッフを支援するに足るだけ COBIT に精通した後で，全員のIT監査スタッフはコントロールモデルと関連する製品に付いての二日間の教育を受けた。試験的に COBIT を使用して，その適用についての優れた洞察と教育を開発するための適切な経験が得られた。

事前監査（予備調査）業務で COBIT は，リスクの高いITプロセスを識別することとITコントロール環境の評価を支援した。COBIT の高いレベルと詳細なコントロール目標に基づいて，組織およびIT方針をレビューすることで，チームは迅速に監査範囲に含むべき領域や潜在的なマネジメントサービスへの助言作業に焦点を当てられた。事前監査で，我々のチームはインタビュー討論を促進するために，COBIT の枠組みとコントロール目標を使用した。データと情報の要件と源泉の識別は，COBIT の情報に対するビジネス要件に参照された。これは，コントロール目標とコントロール方針，手続，標準の検討に際して，監査チームと監査対象者を支援した。

COBIT がコントロール目標とビジネス組織に対する関連する目的に焦点をおいていることは，チェックリスト監査から離れる監査マネジメントの努力を支援した。我々は，COBIT の原則を導入することで，監査計画プロセスとITに対する基礎的なコントロール目標の理解の強化を続ける。

結論

契約の開始時に，監査チームは重要な監査基準の一つとして開始会議において COBIT を参照する。それはレビュー標準に信憑性を加える権威ある源泉である。そして，被監査者と共有するならば，建設的な監査業務の優れた機会を提供する。これは，被監査者に最初からレビューの基礎を理解させることを助ける。さらに，我々のチームは，COBIT の活用は，支援組織委員会（ＣＯＳＯ）と監査基準の最近の変更（つまり，ＳＡＳ７０と７８）にしっかりと組み合わされていることに気付いた。COBIT 監査ガイドラインはまた，監査業務プログラムの開発に使用できる。

COBIT はまた，被監査者が内部統制を評価し，強化することを支援するに有用である。やがてくる監査によく備えるということで，彼等に大きな利益を与える。レビュー基準を認識することは，ITプロセスに対して勧告されているコントロール実務を被監査者を認識していることを意味している。COBIT の構成は，監査人の情報とひきつづく勧告についての要請に関連付け，解釈することを容易にする。

COBIT に関する我々の経験はまた，新入監査人がITプロセスと詳細なコントロール目標の理解し，それを被監査者の組織とIT環境に対して組み立てることを支援した。COBIT を導入することで，一般的な監査ガイドライン，監査手続マニュアルと品質保証レビューを強化し，修正する必要性を確認した。

全面的に，我々は，IT領域，コントロール目標とITコントロールに関する討議についての調和の増大を達成した。

Ad Vannijinatten，パートナー，ＥＤＰ監査，オランダ
Eddy,Schuermans,ＣＩＳＡ，パートナー，保証サービス，ベルギー
Ren' Barlage，ＥＤＰ監査人，クーパー＆ライブランド

要約

オランダのクーパー＆ライブランドは，コンピュータ保証サービスに１００名のＥＤＰ監査を抱えており，その大部分はすでに COBIT について深い知識を持ち，クライアントに対して使用している。多くのクライアントに対して，我々は次のフェーズアプローチを使用している。

・焦点を当てる。ITのビジネス推進者を識別し，ITの展開に含まれるビジネスリスク のレベルを評価する。
・評価 脅威と脆弱性を評価し，欠如または不適切なコントロール対策を識別し，本質的な原因を判定する。

・コントロールの欠陥を評価する。行動計画に合意し，内部統制の改善を適用する。
・モニター　設定された内部統制手段の適切なモニタリングの導入を通じて，継続的な改　善を保証する。

背景

　我々はクーパー＆ライブランドの幾つかのクライアントに対して COBIT を実施し，枠組みの強い支持者である。我々のスタッフは，クライアントのIT部門の改善プログラムの開発にそれを使用している。詳細なコントロール目標は，クライアントのシステム管理プロセスのより良い評価について我々を支援している。

プロセス

　ビジネス状況で COBIT を使用して成功している例を下記に示す。
航空会社　クライアントはIT部門の有効性と効率性を測定するように依頼した。我々はまず，ユーザの満足度を測定し，発見事項を分析した後で，COBIT のガイダンスに基づいて，ITプロセスの詳細なレビューを行った。その結果，IT部門の手続は大幅に改善された。
ネットワークサービス提供者　ネットワーク提供者はITILに基づいたシステム管理を導入していた。我々は第三者レビューを行うように依頼され，結果は提供者のクライアントに報告された。我々のスタッフは，COBIT の枠組みを監査実施に活用した。
非営利団体　COBIT の原則とITILに基づいて，IT部門の改善プログラムを実施した。
商工会議所　幾つかの合併と大きなビジネスの変更が組織のIT環境に影響した。我々は，COBIT の枠組みを適切な改善プログラムの導入に利用した。
銀行　オランダの銀行が幾つかのプラットフォームに対する基本的なコントロールを文書化するように依頼した。我々は，RS／6000，Windows NTサーバーと幾つかのネットワークコンポネントに対する基本的なコントロールを記述した。基本的コントロールのシステム管理の部分で，我々はCOBITの詳細コントロール目標を参照した。
結論

　COBIT のユニークな利益は，ITインフラストラクチャーライブラリー (ITIL) は，COBIT が基礎においている国際的な標準の一つである。英国で開発されたが，ITILは多くの国で一般的である。オランダでは，ITIMF，EDP，ITILユーザグループのメンバーである監査人は，ITIL出版物を使用したITプロセスを監査するようにしばしば依頼されている。COBIT は，その監査を実施するための素晴らしい枠組みを提供している。・

Pratap Oak　上級IT監査人
Jay Stott　副社長 (部長) IT監査
Fidelity Investments　ボストン　マサチューセッツ，米国

要約

　マサチューセッツ州ボストンに本社がある投資管理組織である Fidelity Investments が，COBIT を適用してから，監査業務は著しく一貫しており，現在，コントロール自己評価が可能になった。

背景

　Fidelity は，米国，カナダ，欧州，オーストラリアとアジアの70の市に24，000名の従業員を抱えている。顧客の資産は全体で9，050億ドルである。
　COBIT の枠組みは，革新的にコントロール環境を改善し，付加価値サービスを提供できる。それは，ITシステムを継続的に改善することで全般的なビジネス目標の支援により，我々のCIOやその他の経営者が直面している難題を直接取扱っている。上級マネジメントの支援と継続的改善への激励の結果，監査プロセスを比較的短時間に“COBIT ised”した。
　我々はより少ない資源でより多くの監査を実施し，他の監査グループ，リスク評価，監査計画，監査のスコーピングとの調整と，監査課題のコミュニケーションを改善した。COBIT により得た最も重要な利益は，出力の高い作業を行った満足感であった。

プロセス

以前，ITリスク軽減する難題は最善の慣行と関連する方法論で取扱われていた。我々のマネージャは，継続的改善を強く支持しており，COBIT がIT管理コントロールに対して，一般的に適用でき，受け入れられた標準を提供することをいち早く認識した。COBIT は，Fidelity のビジネスも真財務諸表に直接関連するITコントロールの基礎を提供することで，プロセスを前進させた。

1996年，我々は COBIT の枠組みを使用してレビューを行い，その有用性を確認した。1997年，我々はCOBITドメイン，プロセスとコントロール目標／要素のデータベースを構築した。次に，実施した各種の監査に対して COBIT データベースを適用した。

多くの積極的な変化がこの努力から得られた。監査プログラムと調書のドキュメンテーションは，枠組みに基づいて更新された。COBIT は我々の任務ステートメントに組み込まれた。契約のメモは現在，いかに枠組みを使用するかを説明し，枠組みのコピーは監査に良く備え，監査の利益を理解するために被監査者に利用できる。

結論

COBIT を導入することで，コントロールに関する包括的な主要部を我々の監査に組み込んだ。COBIT はITコントロールに関する権威ある基礎を提供し，完全，効率的かつ一貫したITコントロール環境の網羅を確保することを支援した。

前進することで，我々は COBIT をコントロール自己評価レビューに利用することを計画した。それは，ITコントロール環境の状態についてのよりよい測定基準の基礎を提供し，また，先立つ多くの変化を通して，我々の目標を支援するのに十分な柔軟性がある。

Christyian Hendricks 国防省，米国

要約

米国国防省の監査部（OIG）は，COBIT をIT監査可能な領域を定義する標準として使用している。COBIT はIT社会が理解でき，順守できるように記述されている。その結果，効果的な監査範囲を保証するような戦略計画が作成された。このケーススタディは，IT戦略計画を実施し，監査人のスキルを評価する基礎を確立し，最善のIT訓練コースを選択するためにどのように COBIT が導入されたかを詳述する。

背景

COBIT のドメインとプロセスの枠組みは，コントロール活動を管理でき，定義できる構造で提示している。四つのドメインのそれぞれに対して，コントロール目標はOIGの戦略計画に示された時期に基づいて評価された。我々の長期のゴールは，それぞれのコントロール目標をドメインに含めることである。

プロセス

監査は（COBIT の）コントロール目標を基準として計画された。詳細な監査手続は政府の要求を含む幾つかの領域とコンピュータ支援監査技術の使用に基づいて，開発された。ITで働く監査人は特別な専門知識を必要とするので，我々はスキル評価を実施し，監査がうまく実施されることを保証するために COBIT を使用した。監査人は四つの COBITドメインで作業する能力について，格付けされ，高いレベルのコントロール目標を使用して監査する能力を評価された。それぞれの監査人のITにおける教育，訓練と経験はその三つのスキルのセットに基づいて，特性化された。

基礎的理解：ITプロセス，目的，目標とゴールについての広い知識。

実際の役に立つ知識：ITプロセスにおける内部統制の弱点と強所を識別する実証された能力。

専門家としての知識：内部統制の弱点を識別し，評価し，修正するためにコンピュータ支援監査技術を設計し，使用する能力。

訓練の機会を評価するために，我々は COBIT のドメインとコントロール目標を支援するスキルのセットを提供する能力に基づいて，コースのデータベースを維持している。コースのコスト，スケジュールとパフォーマンスなどの他の要因も考慮された。COBIT コースの評価に基づいて，最善のコースを正しい時期に選択できる。

結論

COBIT はIT社会が理解でき，順守できる枠組みを提供する。その結果，有効な監査範囲を保証する戦略的監査

計画が作成できる。さらに，IT監査と監査人のスキル要件を評価する基礎としてコントロール目標を使用することで，監査を首尾よく実施できることを保証する効果的でタイムリーな訓練を提供できる。

John Beveridge，CISA　ボストンガス会社，米国

要約

COBIT はその利益とそれがどのようにして，ボストンガス会社に利益をもたらすか注意深く研究された。価値を付加する監査サービスを提供するという内部監査部門の戦略と矛盾せずに，COBIT はコントロールの最善の実務のベンチマークとレビューの基準として役立つ。

背景

ボストンガス会社は公益事業であり，1，400名の従業員で年間7億ドルの売り上げがある。米国マサチューセッツ州大ボストン地区の74の市と町に供給している。そのIT環境は，主にIBMKメインフレーム，UNIX，NovelとNTのプラットフォームとネットワークから構成されている。

プロセス

内部監査管理者とIS監査人は COBIT が1996年出版されたときに入手し，すぐにISACAのニューイングランド支部が主催した COBIT の説明会に参加した。

COBIT がボストンガスのIT関連方針と手続の開発およびIT監査の実施に利すると確信したので，その管理者は COBIT の原則をIS部長とISスタッフのメンバーに紹介した。この説明の結果，下記の COBIT のカストマイズされた成功例が明らかになった。

・内部監査部長は，レビューのゴールポストが明確に伝達できるように，COBIT をレ ビューの標準として適用するであろうことを示した。

・IS部門は，COBIT を，現在および将来の機能とプロジェクトを測定するベンチ マーク，コントロール目標のセットとガイドラインとして適用した。

結論

COBIT 導入と，内部監査とIS部門がそれを適用に成功したことは，コントロールの枠組みに通じ，訓練を受け，その原則の実施に時間を割いたことによる。COBIT はITコントロールを強化する一方で，全般的なビジネス目標に重点をおくことで，当社に価値を付加した。

Dvid Abts，執行副社長，MISとオペレーションの取締役
サンタ バーバラ信託銀行 サンタ バーバラ カルフルニア州 米国

要約

サンタ バーバラ信託銀行は，有効なITの管理により全般的なビジネス目標を支援するために COBIT を導入した。

背景

我々はビジネスの必要性に焦点を当てているので，COBIT を採用したそして，真っ先に我々はビジネスを行っている。COBIT の原則を実施することにより，コントロールされた情報システム環境を確保するために必要なステップを取っているので，我々のビジネス目標を追跡することができる。

プロセス

我々のIS監査人は以前，コンピュータシステムとコードの監査に重点をおいていた。COBIT の原則を実施した後で，ビジネスマネージャーにより容易に理解され，支持される監査範囲でビジネスプロセスに従って監査した。例えば，以前“NTに対するコントロール”に焦点をおいていた監査は，現在，“ローンアプリケーションのフロントエンド処理”に目標をおいている。IS監査をビジネスの中断と見なす代わりに，部門のマネージャは現在，監査人の知識を価値の付加と保護に使用している。

ある例では，マネージャは望まない外部者が企業のWWWサイトを通して，内部コンピュータにアクセスできないことを監査人に保証した。しかし，監査スタッフは，eメールの能力があることに気付き，マネージャにeメールシステムは，サーバーを故障させる可能性があるSPAMメールの機会を減少するためにコントロールが必要であることを警戒させた。

結論

COBIT 導入の結果，ビジネスマネージャーとIS監査人の協同は増加し，コミュニケーションは改善された。COBIT 枠組みとその他の要素は，マネージャがどのようにしてコントロールとセキュリティ課題がその部門を利するかを明らかに理解することを支援した。

部門マネージャとIS監査人が同じビジネス言語を話すとき，監査プロセスは銀行全体に利益を与える協同作業となった。

PeterDe Koninck,上級監査人，ブリュッセル，ベルギー
Erik Guldentops,取締役，グロバル情報セキュリティ
Society For World Interbank Financial Telecommunication(S.W.I.F.T)

要約

SWIFTは，COBIT をオランダ，シンガポールと米国にある顧客サポートセンターの監査に使用した。これは，16人･週の監査作業であった。

背景

SWIFTは，ベルギーに位置する2，465銀行によって所有されている銀行間の財務メッセージサービスとインターフェイスソフトウェアの安全確保のための協同組合である。SWIFTの世界的ネットワークは一日約2百50万のメッセージと一日平均トランザクション合計2．3兆ドルを取扱う。

SWIFTの顧客サポート機能は，最近，リエンジニアリングされ，新しいツールとプロセスが置かれた。監査計画は，監査ツールとプロセスに余裕を与えた。COBIT はプロセスを監査するために使用されたが，ツールではなかった。

プロセス

COBITIT管理とコントロールモデルに対する最初のマネジメントの反応は，時期の関係でむしろ否定的（消極的）であった。しかし，被監査者はしばしば監査は悪い時期に来ると考えている。しかし，監査の間，この態度は逆転し，そのアプローチはよく受け入れられるようになった。この変化は監査報告書の草案を上級マネジメントが受取った後で確認された。

マネージャは機密性／インテグリティ／可用性に焦点を当てる伝統的な方法の代わりに使用されたプロセスオリエンテーションに特に感動した。COBIT アプローチの最も明白な結果は，論理的な組立てとインタビューのシーケンスであり，監査人はその知識を適切な順序で組立てるので，プロセスをより効率的にした。

COBIT の枠組みは以前には手を触れていない領域に調査を引入れるので，監査範囲の上級とラインマネジメントと承認を得るために長い討議があった。マネージャはその新規分野で客観的監査を実施する監査チームの能力に疑問を抱いていた。部門は以前はセキュリティを広く定義し，ITセキュリティ課題だけを見ていた。そして，COBIT のアプローチは，プロセスのマネジメントとプロセスのコントロール課題に焦点を当てていた。

我々は，COBIT コントロール目標を使用してマトリックスを構築した。リスク評価は，どの目標を監査の間に検証するかを判定することを支援した。それから，(a) 以前の監査からの範囲，(b) 産業標準，(c) 外部監査人によって提供されたチェックリスト，監査を差し控えた目標をクロスチェックした。マトリックスに基づいて，我々は監査プログラムを構築した。COBIT の枠組みは，COBIT から提供された第一／第二の格付けを使用して監査活動とレビュー対象の領域を優先位づけすることを可能にした。

結論

この包括的な監査に COBIT 枠組みを導入することは，監査人とマネジメントの大きな変化であった。変更はしばしば不幸と批判をもたらすが，プロセスのオリエンテーションは，すばやくマネジメントに正しく評価され，そして監査

人はそれを再び使用するように計画した。

COBIT は，将来の監査にますます使用されるであろう。確かに現在，監査委員会は COBIT をIT監査の参考文献として批准した。それは確かにＳＡＳ７０タイプのレビューの良い基礎と見なされつつある。それとともに，COBIT はまた，企業のIT組織への適用を見出だしている。枠組みを偶然，ふと見出だしたCIO派，それを全てのサービスITマネージャーのために注文した。それはIT組織の測定可能性とプロセス長所を増大するという彼のアイディアと計画を高めた。

COBIT は，また，即時の実務的用途を見出だしている。新しいシステム計画グループに対する使命と目標を定義することへの情報の提供を求めたとき，CIOは私のところにきて，こう言った。“これを行うことを支援するために，君の COBIT 詳細目標を見せてくれないか”私は，ただＰＯ１からＰＯ５までを示すだけであった。彼は使命と目標への情報提供を，もっと前に私に尋ねるべきであった。私自身についてもそのように考えるべきであったのだが。・

COBIT のＦＡＱｓ

１．COBIT の目的は何か。

COBIT の目的は，ITに関連したリスクの理解と管理を支援するためにマネージャとビジネスプロセスのオーナーにIT管理モデルを提供することである。COBIT はビジネスリスク，コントロールの必要性と技術的課題の間のギャップを埋めることを助ける。これは，IT管理の必要性に合致するコントロールモデルであり，情報システムと情報システムのインテグリティを確保する。

２．COBIT を使用するのは誰か。

COBIT はビジネスプロセスと技術に第一の責任のある人，関連し，信頼できるITに依存している人，ITの品質，信頼性とコントロールを提供する人に使用されている。

３．プロセスオーナーは誰か。

COBIT はビジネスプロセス志向であり，従ってまず第一にそのプロセスのオーナーに取り組む。ポーターの一般的ビジネスモデルを参照して，我々は支援プロセス（人的資源，管理，ITなど）同様に，中核のプロセス（購買，オペレーション，マーケッティング，販売など）について話している。その結果，COBIT はIT部門で適用されるべきであると友に，ビジネス全体に適用されるべきである。

上記のアプローチは，今日の企業では，プロセスオーナーはそのプロセスのパフォーマンスに責任があるが，それにはITが統合された部分になっている。換言すれば，それは強化されるとともに，説明できる。その結果，ビジネスプロセスオーナーは，そのビジネスプロセスの境界のなかで展開されているので，ITに対する最終責任を持つ。勿論，彼等は伝統的なIT部門または第三者のサービス提供者のような特殊化された団体から提供されるサービスを使用する。

COBIT は，ビジネスプロセスオーナーに，IT展開の根底にある全ての異なる活動をコントロールすることを可能とする枠組みを提供する。その結果，この根拠か　らITがそのビジネス目標の達成に貢献するという合理的な保証を得ることができる。さらに，COBIT はビジネスプロセスオーナーに，ITサービスの引渡しに関連する異なる団体のなかで，理解と明確さを促進する一般的なコミュニケーションの枠組みを提供する。

４．なぜ，COBIT のオリエンテーションが機能やアプリケーションよりもプロセスに重点を置いているのか。

COBIT の枠組は相互に関連するライフサイクルの活動または相互に関連する別個のタスクに密生する３４のITプロセスから構成されている。プロセスも手は幾つかの理由から選択される。第一に，プロセスは本来，資源使用を最適化しつつ最終結果に重点を置くという方法で，結果志向である。その資源が物理的に構成される方法つまり，部門の人材／スキルは，この観点からはあまり関係がない。第二に，プロセス，そして特にその目標は，本来，より関係があり，組織実体にほど頻繁に変化を大胆に行うことはない。第三に，ITの展開は，特定部門に閉じ込めることはできず，IT専門家に加えて，ユーザとマネジメントも含んでいる。この文脈で，ITプロセスはそれにもかかわらず，共通の分母である。アプリケーションが関連している限り，それは，それは五つの資源カテゴリーの一つとしてCOBIT の枠組の中で取扱われている。従って，要求された情報をビジネスプロセスレベルにもたらす方法で管理され，コントロールされるべきである。この方法で，アプリケーションシステムは COBIT の枠組の統合された部分となり，資源の有利な地点として特別に取扱われる。換言すれば，重点を厳密に資源のみに置くことで，COBIT

目標のアプリケーションのビューを自動的に得ることができる。

5．如何にビジネス要件が強いか。

COBIT のレビュープロセスにおいて，上級マネジメントとCIOは，情報に対するビジネス要件の定義を好み，どのプロセスでどの要件が最も重要かの選択を支持していた。選択は困難であり，プロジェクトの間，専門家の間でかなりの討議を要した。支配的な原則は常に下記であった。このプロセスでこのコントロール目標に対して信頼性に基本的であるのは何か。特別なコントロールを必要とする資源は何か。どの情報要求が特別な注目が必要か。

6．COBIT の全般的な品質はどうか。専門家レビューの一部であるプロセスオーナー／取締役はいるか。

COBIT の最終的な品質を保証するために，いくつかの尺度が採用された。最も重要なものは，

1) 全体の研究プロセスは COBIT 運営委員会（ＣＳＣ）で支配された。成果物をあらかじめ考えることに加えて，ＣＳＣは，その成果物の最終品質にも責任を持っていた。
2) 詳細の研究結果はたえず，品質管理されていた。
3) 枠組同様に，暫定的研究結果はビジネスマネージャーを含む専門家の二つのグループに解説（公開）された。
4) 最終文書を発行する前に，多数の専門家にコメントを求めるために配付された。全般的に，COBIT モデルはビジネスマネジメントに全体として興味を持たせ，ITへのコントロールを改善するという観点からその付加価値を評価していることを経験は示している。この観点から，顧客の満足度以上に，要求された品質が達成されたという確信を持っている。

7．COBIT の将来方向は何か。

どのような包括的かつ草分けの研究と同様に，COBIT は3～5年後とに更新されよう。これはモデルと枠組が包括的であり，有効であることを保証する。検証は，また，３６の主要な参照文献が変更されていないこと，もし変更されていたならば，ドキュメントに反映することの保証を伴う。

8．COBIT を特定の監査結論のステートメントの基準として使用できるか。

そのとおり。コントロール目標の監査ガイドラインに基づくことは，監査人の意見を監査結論それを権威ある基準に置き換える。（注．原文には重複した記述があり，誤植と思われる。従って，訳出不能）COBIT は全世界の基準設定団体（公的および民間の）からの３６の基準とITに対する最善の実務文書に基づいている。それには，欧州，カナダ，オーストラリア，日本および米国からの文書を含んでいる。COBIT はその時点で識別できる全ての関連する世界的基準を含んでいるので，ITコントロール基準として全てを包含している。その結果，COBIT は監査におけるITコントロール基準を提供する権威ある参照文献として使用できる。

9．どのようにして，ＩＳＡＣＦ／Ａは，主要な参考文献のリストを決定したか。

主要な参考文献のリストは，COBIT 運営委員会，研究，専門家のレビュー，品質保証に参画した専門家の知識，スキルと能力に基づいて，共同の合意として開発された。

１０．コントロール目標は，コントロールの最低のレベルを意味するのか，または最善の実務を意味するのか。

我々はなお，コントロール目標のレベルであり，コントロールガイドラインやコントロール実務のレベルになっていないので，最低限であり，同時に最善の実務である。企業の環境，特定のビジネス目標，達成したいと望んでいるセキュリティのレベル受容しようとしているリスクの度合いなどが，全てプロセスのコントロール目標が正しいレベルのコントロールに翻訳されるかを決定するこれは，COBIT プロジェクトのさらなるフェーズで取扱われるであろう。

その選定の全ては自明ではなく，コントロール選択のプロセスは厄介な，時間のかかるものであるので，標準の最低限のセキュリティとコントロールレベルは確かに開発し，促進しなければならない。

１１．プラットフォーム特定のコントロールの欠如はどうなるか。

COBIT コントロール目標は一般的な性質であり，ITプロセスの内部監査の活動やタスクを取扱う。この方法でプラットフォームに独立である。一方，しかし，それは全般的な構造であり，それはより特定のプラットフォームに関

連したコントロールを定義しなければならない。事実，全般的なコントロール目標は，それが例えば，メインフレームのプラットフォームであろうとOAプラットフォームをコントロールするものであろうと妥当なものでなければならない。ある局面では，与えられた環境により重点を置く必要があることは明白である。

12．アプリケーションコントロールはどこにあるか。

アプリケーションコントロールは COBIT モデルに完全に統合されている。このオプション（選択）は，COBIT はビジネスプロセス志向であり，このレベルでアプリケーションコントロールは単に情報システムと関連する技術に作用する全般コントロールの一部であることを考慮している。しかし，多くの場合，この部分はアウトソーシングできない。従って，“アプリケーションコントロールはどこにあるか”という質問は非常に重要である。

アプリケーションとデータは，COBIT 枠組で五つの資源カテゴリーのうちの二つとして扱われている。それは，ビジネスプロセスレベルで要求された情報を伝えるものである。この方法で，アプリケーションシステムとデータは COBIT 枠組の統合された部分であり，資源の有利な条件を通じて，特別に取扱われる。これを行うことで，多くの COBIT プロセスはアプリケーションコントロールを取扱い，受領からオペレーションまでの全てのライフサイクルを通じて，これは続けられる。

全体的な資源のレビューの他に，“データを管理”する一つのプロセスがあり，そこでは，伝統的なトランザクションとファイルのコントロールが見出だされる。それにもかかわらず，自己のそれに対するコントロールが効果的にアプリケーションシステムとデータをコントロールするには十分ではないことを考慮すべきである。

自己の組織に COBIT を統合するとき，上記の要素を考慮すべきである。この点に関して，一般的なコントロール目標に対して，プラットフォームに特有のコントロールを追加することが要求される。プラットフォームはこの意味で広く解釈すべきであり，（つまり，OA，通信，データウェアハウスなど）この点で再訪問されるべき COBIT プロセスは，“技術”資源カテゴリーに関連するものである。

13．コントロール目標に重複があるのは何故。

しばしば起こることではないが，コントロール目標の重複は意図的なものである。あるコントロール目標はドメインとプロセスを超越し，従って，それが各ドメインまたはプロセスに存在していることを保証するために，繰り返さなければならない。あるコントロール目標はお互いにクロスチェックすべきことを意味し，従って，二つ以上のドメインまたはプロセスに一貫して適用することを保証するために繰返サなければならない。こうして，重複と考えられるが，COBIT はそのITコントロールの適切な適用範囲を保証するために意図的に繰り返されている。

14．コントロール目標は監査ガイドラインに結合されているか，またその程度は。

マネジメントはITをコントロール下に置く課題を如何に取扱うべきかについての革新的な助言を求めているので，目標はプロセス志向で開発されている。コストとリスクをバランシングすることは取扱うべき次の課題である。（つまり，それぞれのコントロール目標をどのようにまたは実施すべきかの自覚した選択を行うために）革新原則はそのまま残るが，将来の COBIT 製品は，完全にこの選択を取扱う，コントロール目標はまず情報コントロール基準（有効性，効率性，機密性，可用性，インテグリティ，準拠性と信頼性）を達成するために適用すべきである。その結合はプロセスである。コントロール目標は，マネジメントがプロセスに対するコントロールを確立することを支援し，監査ガイドラインは，ビジネス目標を達成するために必要な情報要求が充足されるように，プロセスが実際にコントロール下にあることの保証を提供することで監査人や評価者を支援する。ウォーターフォールモデルで表現されたコントロールの枠組に関して，監査ガイドラインはコントロールプロセスからビジネス目標にフィードバックを提供するものと見なされる。コントロール目標は，ITプロセスをコントロール下におく，ウォーターフォールを下るガイドである。監査ガイドラインは，課題とともに，ウォーターフォールをさかのぼるガイドである。ビジネス目標が達成されたという保証はあるだろうか。ときには，監査ガイドラインは，コントロール目標からの間違いのない翻訳である。よりしばしば，ガイドラインはプロセスがコントロール下にあることの証拠を求める。

15．コントロール目標にリスクのステートメントがないのは何故か。

リスクステートメントの条項は初期の COBIT プロジェクトの研究とレビューの局面で真剣に考慮され，検討されたが，マネジメントは対応的アプローチ（リスクは緩和される）よりも革新的なアプローチ（目標は達成される）を選択したので，残されなかった。リスクアプローチは，コントロールを実施しないときのリスクが実証されたときに監査ガイドラインの終わりに到来する。COBIT の適用において，マネジメントがどのコントロールを実施すべきかを決定し

たとき，監査人がどのコントロール目標をレビューすべきかを決定したときにリスクアプローチは確かに有用である。その意思決定の双方は，全くリスク環境に依存する。

16．COBIT の使用に関してどのような訓練が利用できるか。

ISACAの国際本部を通じて，COBIT の基礎とマネジメント，監査人と評価者の使用法に関する一日から二日の講習会がある。訓練は，COBIT の枠組，定義，コントロール目標，監査ガイドライン，ケーススタディと成功する導入のアプローチを網羅する。訓練は執行マネジメント，ユーザまたは評価者の好みに合わせて，誂えられる。さらに，ISACAは，COBIT の認識，その枠組，定義，コントロール目標と監査ガイドラインを提供する展示スライド（CD－ROMディレクトリーに“PPスライド”として，含まれている。）を作成している。ISACAはまた，米国監察長官監査人訓練研修所で年間を通じて，二日の COBIT コースを提供している。ISACAは，どのような組織の要求にもまた要求される詳細度に対してもプレゼンテーションを誂えられる。

17．組織の誰が訓練を受けに行くべきか。

COBIT の訓練は，マネージャ。ISと監査のマネージャ，IT専門家，ビジネスプロセスマネージャー，品質保証と監査専門家が出席すべきである。

18．要求される訓練のレベルはどれくらいか。

必要な訓練の量とレベルは，製品について人がどのように心地好く考えるかの関数である。より革新的な，そして，IT部門との関係を良く定義している組織では，訓練は単に COBIT の導入ツールセットを利用することで充足される。しかし，物事が十分に定義されていない実体では，マネジメント，ITと監査からISACAの一日の講習会に出席することが強く奨励される。それは，国際本部または全世界の支部を通じて利用できる。

19．詳細コントロール目標とコントロール考慮事項に差異があるのは何故か。

詳細コントロール目標とコントロール考慮事項に差異があってはならない。コントロール考慮事項と同じ用語が詳細コントロール目標には現れないこともあるが，しかし，コントロールの考慮事項の課題はコントロール目標で取扱わねばならない。

20．COBIT を使用するようにITマネジメントをどのような方法で示唆すべきか。

ITの最適な責任を概観することを支援するために，また，どの部門がコントロールされるべきかのベンチマークを確立するように COBIT 枠組の使用を示唆するであろう。ITが何を取扱うかだけではなく，それに何を期待すべきかを知ることは上級マネジメントにとって，しばしば非常に価値がある。

21．COBIT の枠組は他の受け入れられているコントロールモデルよりも優れているか。

多くの上級マネジメントは，例えば，COSO，カドベリー，COCOまたはKingなどの信用上の責任に関連して，一般的なコントロール枠組の重要性を認識している。しかし，それぞれの詳細について認識しているとは限らない。さらに，マネジメントは高いレベルのより技術的なセキュリティガイドライン，例えば，OECDとIFACITステートメントや，詳細レベルでの実務のDTIコードをますます認識している。前述のモデルはビジネスコントロールとITセキュリティ課題を強調しているが，COBIT のみがビジネスの観点からIT特有のコントロール課題を取扱おうとしている。COSOがビジネスモデルの源泉資料として使用されていることに留意すべきである。最後に，COBIT はそのコントロールモデルに置き換わろうとしているのではない。それは，IT環境でより詳細を提供することを意図しているが，それらモデルの長所の上に構築されている。

22．COBIT をITマネージャーに売り込む最も速い，かつ最善の方法は何か。

我々全てが知っているように，救援の騎兵隊はない。導入ツールのその他のものが指摘しているように，組織分化は致命的に重要である。革新的文化は，そうでないものと比較して，より感受性が高い。しかし，ビジネス局面に重点を置くことと COBIT は技術的術語を失っていない事実を考慮すべきである。さらに，COBIT はITマネージャーが考える方法で設計され，その最大の利益は全てが一か所で文書化されていることであることを指摘すること。

23. COBIT **とその枠組はCIOに受け入れられているか。**

しかり。それは世界的に多くの組織で受け入れられており，新しいケースが文書化されている。しかし，その実体ではCIOが COBIT **を活用可能なIT枠組として受け入れている驚くべきことではない。監査および／またはIT部門のなかでの** COBIT **の一つ以上の擁護者の直接的な結果である。**

24. COBIT **との** COBIT **の討議において，主要なセールスポイントは自己評価とベンチマーキングである。ISACAの将来計画は。**

COBIT **の運営委員会はあなたのCIOS完全に合意する。他の** COBIT **の購入者から多くの同様のコメントを受けているからである。**COBIT **の枠組が最初に構築されたとき，結局は，重要成功要因，重要パフォーマンス指標とベンチマーキングと評価の測定を含むマネジメントガイドラインを発行する計画があった。ISACAは現在，評価ガイドラインを開発し，テストするプロセスを始めている。この製品の最初のフェーズは1999年の前半に発行する計画である。**

25. COBIT **は現在，関連するビジネスリスクを取扱っておらず，しかし，達成すべきより革新的なコントロールステートメントを取扱っているが，リスク識別の想定される必要性を取扱うことに考慮が払われているか。**

前述の質問の一つで取扱っているように，それはマネジメントによってあまりにも対応的であるの考えられたので，リスク評価の条項は最初のフェーズに残されなかった。COBIT **のファミリーの製品，自己評価，モデルの次のフェーズ発行は，定量化されたリスクステートメントの使用を包含することに近くなろう。その教材が利用できるようになるまで，ある形式のビジネスリスク評価が導入の尺度（コントロール目標P09参照）を定義するためにマネジメントによって活用されよう。監査人はまた，レビュー対象のプロセスとメインフレームとコントロール目標を選定するとき，ある形式のビジネスリスク評価を行うであろう。**

COBIT **導入のツールセットの付録**

下記の付録を見るために，あなたのシステムにインストールされている Adobe Acrobat Reader **がなければならない。必要であれば，リンクをアクティベートしようとする前に，このユーティリティをCD－ROMからあなたのシステムにインストールして下さい。導入ガイダンスのための“**AAReader**”ディレクトリーのREADME.TXTファイルを見て下さい。**