COBIT™
監査ガイドライン

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

利用上の注意

情報システムコントロール財団と CobiT のスポンサーは，「情報システムおよび関連技術のための内部統制目標(Control Objectives for Information and Related Technology)」製品をを主に内部統制専門家のための教育用資料として作成した。情報システムコントロール財団とそのスポンサーはこの使用による結果がすべて成功を納めることを保証するわけでない。この製品はすべての適切な手続きとテストを包んでいるわけではない。また，同じ結論を得るための合理的に指示された他の代替手続きやテストを排除するものでもない。内部統制専門家は手続きやテストが適切であるかどうかを決定する際に，特定のコントロール環境に対する特定のシステムまたは情報技術に向けられた環境についての専門家としての判断を下すべきである。

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 0-9629440-6-8 (監査ガイドライン)
ISBN 0-9629440-3-3 (CD-ROM 付き 5 分冊)

印刷：アメリカ合衆国

監査ガイドラインの紹介

COBITと*監査ガイドライン*

*監査ガイドライン*は，監査と評価を実施する際に，COBITの*フレームワークとコントロール目標*を容易に適用できるようにするための補完的なツールである。*監査ガイドライン*の目的は，COBITスキーム全体に適合できる一般に認められている監査慣行に基づいて，コントロールを監査し評価するために容易な構造を提供することにある。

個々の監査の目標と慣行は組織によってかなり異なっており，また，外部監査人，内部監査人，評定者，品質レビュー者，技術評価者などの多くの実務家が監査関連の活動に関与している。したがって，*監査ガイドライン*は構成上，概括的かつ高レベルなものとなっている。

監査人は，管理者やビジネス・プロセス・オーナに対して，組織内のコントロールを保証し助言したいという欲求を総じて持っている。すなわち，関連する*コントロール目標*の達成を合理的に保証すること，それらのコントロールのどこに重大な弱点があるかを明らかにすること，それらの弱点によって引き起こされる可能性のあるリスクを立証すること，そして最終的に取るべき是正措置について経営陣に助言することである。COBITは，情報と関連技術のセキュリティとコントロールについて明確な方針と良い慣行を提供している。それゆえに，*監査ガイドライン*の基礎を確実に*コントロール目標*に置くために，監査結果から監査人の意見を取り出し，それを権威ある判断基準（世界的な民間および公的な標準化団体からの36の標準と最良の慣行についての記述）に置換えている。

*この監査ガイドライン*は，COBITの*フレームワーク*と詳細な*コントロール目標*と共に統合された監査計画を作成するための指針を提示している。*監査ガイドライン*はCOBITの*フレームワーク*や*コントロール目標*と共に使用すべきであり，特定の監査計画への展開が可能である。しかしながら，*監査ガイドライン*は網羅的なものでもなく，また決定的なものでもない。また，すべての人にとって完璧なものではなく，それぞれの環境に合わせる必要も有り得る。

以下の4点はガイドラインの主旨とは異なる事項である。

1. *監査ガイドライン*は，過去の弱点，組織に対するリスク，周知の小事件，新規の開発，および戦略的選択など広範囲な要素までも考慮した総合的な監査計画作成ツールを意図して作成されてはいない。*フレームワークとコントロール目標*は方向性を示してはいるが，具体的な活動についての手引きは，*監査ガイドライン*の範囲外である。
2. *監査ガイドライン*は，一般の監査およびIT監査について一般的に認められている基礎を取り入れているが，監査の基本を教えるためのツールを意図してはいない。
3. *監査ガイドライン*は，コンピュータ化された企画，評価，分析および文書化のためのツール（コンピュータ支援監査技術を含むが，それのみにとどまらない）が，ITプロセスの監査の支援と自動化にどのように使用できるかを詳細に解説してはいない。情報技術は監査の効率性と有効性を高める巨大な潜在能力を有するが，このトピックスに関する紹介も*監査ガイドライン*の範囲外である。
4. *監査ガイドライン*は網羅的なものではなく，また決定的なものでもない。ただし，COBITおよびCOBITの詳細化された*コントロール目標*と共に発展する。

COBITの*監査ガイドライン*によって，監査人は個々のITプロセスをCOBITの推奨する*コントロール目標*と対比して検討し，コントロールの何処が十分かを管理者に保証するのを支援し，またプロセスの何処が改善を要するか

を管理者に助言することができる。

プロセス・オーナは，管理者の観点から「自分がしていることは万全か，またもしそうでなければ，どのように改善するのか」という質問を投げかけるであろう。COBITの*フレームワークと監査ガイドライン*は，これらの質問に答えるのに役立つであろう。この方法は「受動的」な観点を示しているが，一方で，監査人はまた「率先垂範的」な方法で管理者を支援しなければならない。*フレームワークと監査ガイドライン*は，どちらもプロセスとプロジェクト開発の初期の段階において，「改善する必要がないと思っているのに一体何をしなければならないのか」という質問に対し積極的に答える時に適用可能である。

監査ガイドラインの一般構造

コントロール評価のための最も一般的なモデルは，監査モデルである。また最近よく採用されつつある方法は，本解説の終わりの部分に掲載しているリスク分析モデルである。コントロールの評価に関与している人は皆どちらかのモデルを活用できる。

監査の目標は，

・管理者に*コントロール目標*が達成されつつ有ることを合理的に保証すること
・重大なコントロールの弱点がある箇所を指摘し，そのリスクを立証すること
・是正措置を管理者に助言すること

である。

一般的に認められている監査プロセスの構造は，次のとおりである。

・識別と文書化
・評価
・準拠性テスト
・実証性テスト

したがって，ITプロセスの監査は以下のように実施する。

► ビジネス要件に関連したリスクと関連するコントロール措置を**理解する**
► 表明されたコントロールの適切性を**評価する**
► 表明されたコントロールが，その通り一貫して継続的に機能しているかどうかをテストすることにより準拠性を**査定する**
► 分析的手法を使用したり，代替資料を調べることにより，コントロール目標が達成されない時のリスクを**実証する**

保証について助言する形での管理者支援を目的として，我々はこの構造をCOBIT要件に基礎を置く監査*フレームワーク*に展開した。

・階層化アプローチ（レベル）による表現
・ビジネス目標指向
・プロセス重視
・焦点の対象
　－管理すべき資源
　－必要な情報基準

最も高いレベルにおいては，この一般的な監査方法は以下により支援される。

・COBIT *フレームワーク*，特にITプロセスの分類や適用可能な情報基準やIT資源に関する要約の部分（COBIT *コントロール目標*のサマリー・テーブル参照）
・監査プロセス自体の要件（8ページの監査プロセス要件を参照）

・ITプロセス監査の一般要件（10ページの一般*監査ガイドライン*を参照）
・コントロールの一般原理（8-9ページのコントロール・プロセスの観察を参照）

第二のレベルは，本書の本論であるが，各ITプロセスに対する詳細な*監査ガイドライン*から構成される。
これらのガイドラインは，理解，評価，査定，実証の一般的構造に従う標準のテンプレートで表現されている。このテンプレートは，一般的なITプロセス*監査ガイドライン*や*詳細監査ガイドライン*にも適用される。

第三のレベルすなわち最下位のレベルでは，監査人は監査計画策定の局面で，詳細なコントロール目標に影響を与える下記の監査上の留意点を考慮しながら，個々の諸条件を満たすように*監査ガイドライン*を補足する。

・部門特有の基準
・業界標準
・プラットフォーム特有の要素
・採用された詳細なコントロール技法

このレベルで重要なことは，コントロール目標が常に何処にでも適用できるとは限らないことである。
従って，高レベルのリスク評価を行って，どの目標に特に焦点を当て，どの目標は無視するかを決定することを薦める。

これらすべての要素は，IT監査の計画策定や実施に役立つし，また，詳細な監査ガイドラインをより良く統合して適用する場にも役立つよう提示されている。ただし，ガイドラインは完全なものではなく，またすべてに適用できるものでもない。高レベルの支援情報（一般ガイドライン，監査プロセス要件，コントロールの監視）は，監査人が必要な監査手続書を作成する時に役立つであろう。

監査ガイドラインを適用するための詳細な構造	
レベル1 **一般的なIT監査アプローチ**	► **COBIT *フレームワーク*** ► **監査プロセス要件** ► **コントロール目標** ► **一般*監査ガイドライン***
レベル2 **プロセス監査ガイドライン**	► **詳細な*監査ガイドライン***
レベル3 **詳細なコントロール目標を補足する** **監査上の留意点**	►**個別条件** **・部門特有の基準** **・業界標準** **・プラットフォーム特有の要素** **・採用された詳細なコントロール技法**

監査プロセス要件

何を監査し何を保証をするのかを明確にした後は，監査業務を遂行するのに最も適切な方法または戦略を決定しなければならない。最初に，*適切な監査範囲を決定する*必要がある。そのためには以下についての調査，

分析，定義が必要である。

- 関連するビジネス・プロセス
- 他のプラットフォームまたはシステムとの相互接続性のみならず，ビジネス・プロセスを支援しているプラットフォームと情報システム
- 内製またはアウトソースされているものを含め，ITの役割と責任の定義
- 関連する業務リスクと戦略上の選択

次のステップは，特にビジネス・プロセスに関連する*情報要件を明らかにする*ことである。そして，ビジネス・プロセスに関連する可能性のあるあらゆるレベルのコントロールのみならず固有のITリスクを明らかにする必要がある。これを達成するために，次の点を明らかにすること。

- ITに影響を与えるようなビジネス環境の最近の変化
- IT環境，新規開発などに対する最近の変化
- コントロールやビジネス環境に関係する最近の出来事
- マネジメントが適用したITモニタリング・コントロール
- 最近の監査や認証の報告書
- 自己査定の最近の結果

これらの入手した情報に基づいて，関連するCOBITプロセスおよびそれらのプロセスに適用される資源を選ぶことができる。このため，プラットフォームまたはシステムが異なる度に，あるCOBITプロセスをその都度監査する必要が生じてくるであろう。

詳細な監査計画をさらに緻密なものにしなければならないという基本的な考え方を基に，例えばコントロールに基づく方法でいくのか，あるいは実証的な方法で行くのか，監査戦略を決定する必要がある。

最後に，監査を実施するためにすべてのステップ，作業，判断する時点を考察する必要がある。標準テンプレートに従った一般的な監査プロセス（ステップ，作業，判断する時点を含む）の例が，付録IVに示されている。

監査プロセス要件

・ 監査範囲の定義	► 関係するビジネス･プロセス ► そのプロセスを支援しているプラットフォーム，諸システム，およびそれらの相互接続性 ► 役割，責任，および組織構造
・ ビジネス･プロセスに関連する情報要件の明確化	► ビジネス･プロセスとの関連性
・ 固有のITリスクと全レベルのコントロールの明確化	► ビジネスおよび技術環境における最近の変化と出来事 ► 監査，自己査定，認証の結果 ► 管理者が適用したコントロールの監視
・ 監査対象のプロセスとプラットフォームの選定	► プロセス ► 資源
・ 監査戦略の設定	► コントロール X リスク ► ステップと作業 ► 判断する時点

一般的なIT監査ガイドライン

10ページのテンプレートは，ITプロセス監査のための一般的要件を示しており，通常すべてのプロセスに適用できる*監査ガイドライン*の第一レベルを規定する。このテンプレートは，主としてプロセスの理解と主幹部署の決定を目的としており，すべての詳細な*監査ガイドライン*の基盤となり，参照して使えるフレームワークとなるべきものである。

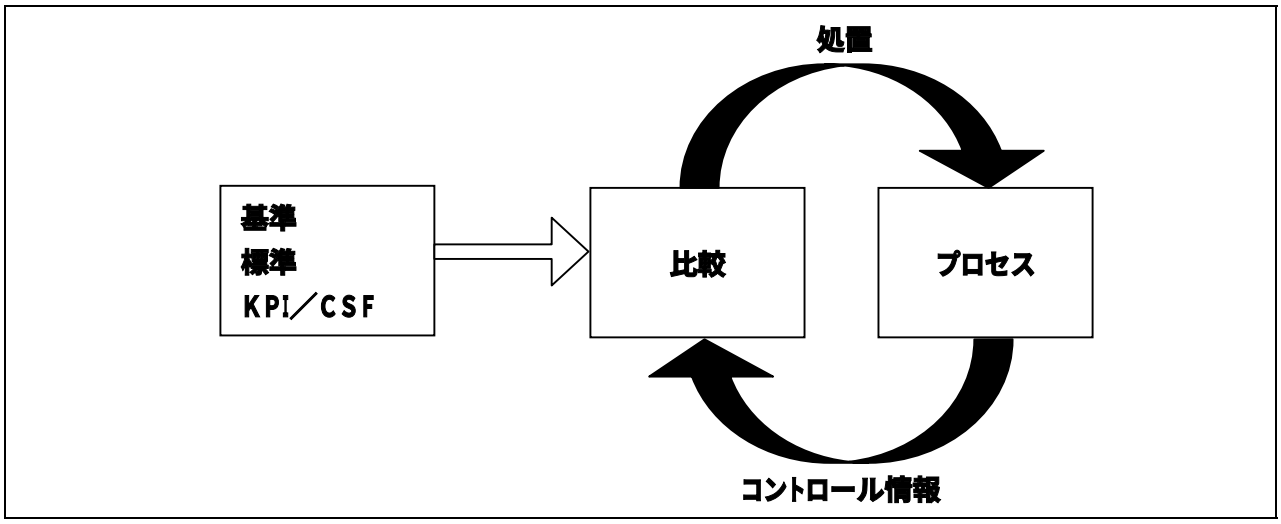
これと同じテンプレートは，COBIT *フレームワーク*に示されている34のプロセスに適用されている。

コントロール･プロセスの観察

コントロールの一般的な原理は，*監査ガイドライン*をさらに補う方法について別の考え方を提供してくれる。これらの原理は，主としてプロセスとコントロールの責任，コントロール標準，およびコントロール情報の流れに焦点を当てている。

コントロールは，マネジメントの視点からすれば，何が達成されつつあるかを決定することとして定義される。つまり，活動実績を評価し，必要ならば業績が計画どおりに達成されるように是正措置を取ることである。

コントロール･プロセスは，4つのステップから構成される。第一に，プロセスに対して要求されるパフォーマンスの基準を明示すること。 第二に，プロセスの中で起きていることを検知する手段を有すること。つまり，当該プロセスは，コントロール部門にコントロール情報を通知すること。第三に，コントロール部門はその情報を標準と比較する。第四は，実際に起きていることが標準に従っていないならば，コントロール部門は是正措置を取るよう指示し，情報をプロセスに送り返す。



このモデルについて，以下の観点からコントロールを観察すれば監査に有効である。

1. このモデルが機能するためには，ビジネス（あるいは，この場合IT）プロセスに対する責任が明確でなければならない。しかも，会計責任も明確でなければならない。 さもなくば，コントロール情報は流れず，是正措置は取られないであろう。

2. 標準は非常に広範囲にわたっており，高レベルの計画や戦略といったものから，詳細に測定可能な重要業績指標（KPI）や重要成功要因（CSF）まで含む可能性がある。明確に文書化され，保守され，伝達されている標準は，良きコントロール・プロセスに不可欠なものである。これらの標準を管理する責任の明確化も，また良きコントロールの要件である。

3. *コントロール・プロセス*の要件も同様である。すなわち，明確な責任を伴ってそれがどのように機能するのかが明確に文書化されている必要がある。重要な点は，標準からの乖離，つまりどのくらい標準からずれていいのかその限界が明確に定義されていることである。

4. *コントロール情報*の適時性，完全性，適切性，並びにその他の情報も，コントロール・システムが良く機能するための基本であり，監査人が取り上げなければならないことである。

5. コントロール情報と是正処置情報は，共にある事象が発生した後の会計責任を*立証する*際の証拠として必要である。

一般監査ガイドライン

理解

コントロール目標を達成するための活動を文書化し，表明されたコントロール対策/手続を明確にするための監査手続き実施

適切な管理者やスタッフと面接して以下について理解する。

- ビジネス要件と関連するリスク
- 組織構造
- 役割と責任
- 方針と手続
- 法律と規制
- 実施中のコントロール対策
- 管理者の報告（状況，業績，行動項目）

検討中のプロセスによって特に影響を受けるプロセス関連のIT資源を文書化する。

検討中のプロセス，プロセスの重要性能指標（KPI），並びにコントロールの意味が，例えば，プロセスのウォーク・スルーを実施して見て，理解されているかを確認する。

コントロール評価

実施中のコントロール対策の有効性やコントロール目標の達成度を評価するための監査手続き実施。基本的に何をどのようにテストするか否かの決定。

レビュー中のプロセスに関するコントロール対策の適切性を評価するが，このとき明らかにされた標準，業界標準慣行，コントロール対策の重要成功要因（CSF）を検討し，監査人は専門家としての判断を下す。

- 文書化されたプロセスの存在
- 適切な成果物の存在
- 責任と会計責任が明確で効果的
- 必要に応じ，補完的コントロールの存在

コントロール目標の達成度合いを判定する。

準拠性評価

確立されたコントロール対策が規定された通りに終始一貫し継続して機能していることを保証し，コントロール環境の適切性を判定するための監査手続き実施。

選定された項目/期間に関して直接的および間接的な証拠を入手し，それらを使用し検討期間中，手続きが遵守されているかを確認する。

プロセスの成果物の適切性について限定した範囲でレビューを行う。

ITプロセスの適切性を保証するのに必要な実証性テストのレベルと追加作業を決定する。

リスクの実証

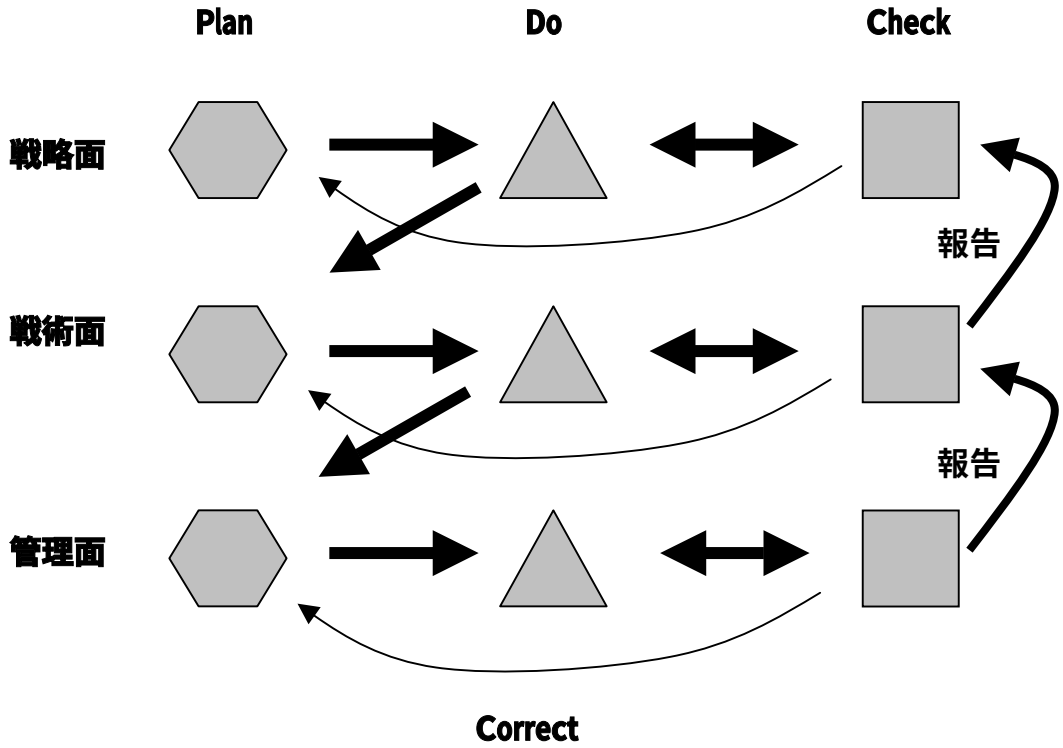
分析手法や参考となる代替情報を使い，コントロール目標が達成されなかった場合のリスクを実証するための監査手続き実施。

目標は意見を支持し，管理者に対策を取るよう警告することである。監査人はこのように重要で機密性のある情報を，創造性をもって見出して説明しなければならない。

コントロールの弱点，それによる脅威と脆弱性を文書化する。

例えば，root-cause分析を使って顕在的および潜在的な影響を明らかにし文書化する。

例えば，ベンチマークを実施し比較情報を示す。



コントロールは，管理者が好む伝統的なPlan－Do－Check－Correctのサイクルの様々なレベルにおいても機能する。このモデルは次のようなものである。

・plan－do－checkという論理的な順序が取られるが，必要に応じ順序を変更する
・戦略面，戦術面，管理面の各レベルでどのようにこのことが起こるか
・いくつかの垂直方向，水平方向の関係
　－戦略面のDoが戦術面のPlanに帰着する
　－戦術面のDoが管理面のPlanに帰着する
　－CheckとDoの活動が継続的に協調しながら実施され相互に影響しあう
　－管理面のCheck活動の報告が戦術面のCheckに対して行なわれ，戦術面のCheck活動の報告が戦略面のCheckに対して行われる

コントロールのメカニズムを評価する時，これらの異なるレベルにおいてコントロールが機能すること，および，それらは複雑な関係にあるということを，レビュアーは知らなければならない。

COBIT のプロセス指向は，様々なコントロールのプロセス，レベルや相互関係について様々な考え方を提供しているが，コントロール・システムの実際の導入や評価には，ここで付け加えられた様な複雑な面を考慮する必要がある。

すべてを組み合わせる

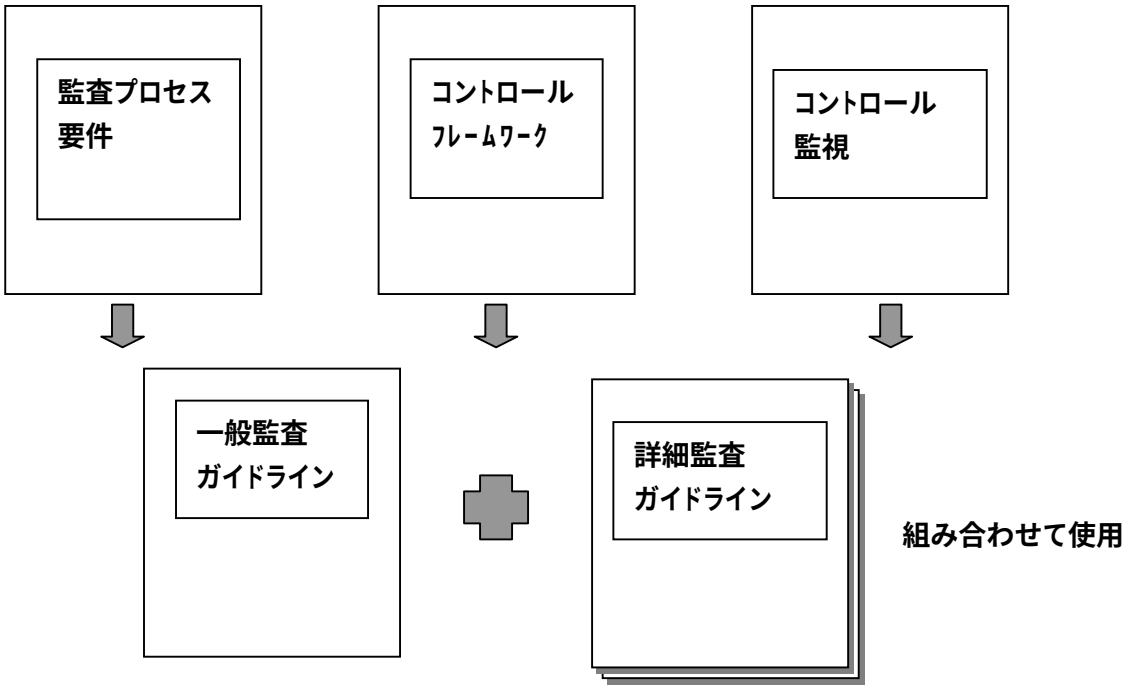
要約すると，詳細な*監査ガイドライン*は常に一般ガイドラインと検討中のプロセスを考慮することによって補完され得るし，また監査目標を達成するために更に監査作業を設定することができる。
監査プログラムの作成それ自身は，IT 監査プロセス要件，COBIT *フレームワーク*，高レベルの*コントロール目標*，および上記のコントロールについての考慮点が役に立つ。

コントロール目標と監査ガイドラインとの連携

当諸目標はプロセス指向から発展して来た。それは，管理者がITを管理下に置く際の課題をどう処理するかについて積極的な助言を求めているからである。*コントロール目標*は，管理者がプロセスに対しコントロールを設定するときに役に立つし，*監査ガイドライン*は，プロセスが実際にコントロールされていて，ビジネス目標達成に必要な情報要件が満たされるであろうことを監査人あるいは評価者が保証する時に役に立つ。

この2つを関連づけているのはプロセスであり，それゆえに*監査ガイドライン*は各コントロール目標に対するものとは対照的に各プロセスに対して作成されてきた。

ウォーターフォール・モデルによって表現されるコントロール・フレームワークに関しては，*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さかのぼってフィードバックを提供していると見ることもできる。コントロール目標は，ウォーターフォールを下っていき， IT プロセスをコントロール下に置くための指針になる。 *監査ガイドライン*は，「ビジネスの目標が達成されるという保証があるのか」という疑問についてウォーターフォールを支援するための指針となる。時には，*監査ガイドライン*は*コントロール目標*を直接言い換えたものになる。また多くの場合，監査ガイドラインはプロセスがコントロール下にあるという証拠を探し求める。



評価作業のための機会と挑戦

監査／評価作業の基本として，*フレームワーク，コントロール目標*並びに*監査ガイドライン*を使用することには，幾つかの明確な利点がある。

- 第一レベルと第二レベルの情報基準の使用により，検討対象の監査活動並びに監査分野に対して優先順位づけが可能になる。
- フレームワークあるいはモデル無しには，通常取り扱えないような分野の調査を実施できる。
- 監査人は，インタビューする時のより論理的な構成や順序をプロセスに沿って自分なりに展開できる。
- どのプロセスにおいてはどの資源がより重要かという指標を用いて調査に集中できる。

・次の事項を保証する戦略的な監査計画に対して，監査可能なIT分野を定義するための標準となる。

－効果的な監査範囲

－必要な監査技術の適時な習得/確立

しかしながら，フレームワークと目標を監査業務に統合するには，いくつか乗り越えなければならないことがある。

・変革は容易ではない（取り組み姿勢，ツール類，技術，……）

・検討対象領域のコントロール目標の完全性と適合性をチェックする時は，最初から詳細なレベルまで適用することは厄介である。

・*監査ガイドライン*では，必要なだけ同じ内容が繰り返されているが，これはコントロール目標とコントロールのメカニズムの間には，1対1の関係となることは殆ど無く，1つのメカニズムが複数の目標に対応するのに役立ったり，1つの目標を達成するのに複数のメカニズムが必要になったりするからである。

・不必要とも思われるある種の形式にこだわること（例えば，バックグラウンド情報の記録）を強制している。

もう一つの評価方法としてのリスク分析

コストとリスクのバランスをとること，すなわち，各コントロール目標をどのように具体化するのか否かを意識して選択することが，次の課題である。 リスク分析方法は，前進的な原則が残っているが，この選択を取り扱うものである。情報のコントロール基準（有効性，効率性，機密性，可用性，インテグリティ，準拠性および信頼性）を達成するためには，まずコントロール目標を適用すべきである。 実施すべき対策を決定する際に，管理者がある種の業務リスク評価を使用する必要が有ることは自明である（CO P09参照）。 監査人は，レビューのためにプロセス領域やコントロール目標を決める時にもある種のリスク評価を行う。

ITのリスク分析として，一般に認められている方法を以下に示す。

このモデルにおいては，先ず資産の評価がなされる。 資産の評価は，COBIT *フレームワーク*の中でビジネス目標の達成支援に必要な基準を含む情報から成る（その情報を生み出すために必要なすべての資源も含む）。

次のステップは脆弱性の分析†であり，レビュー対象のプロセスにおける情報基準の重要性を考察する。

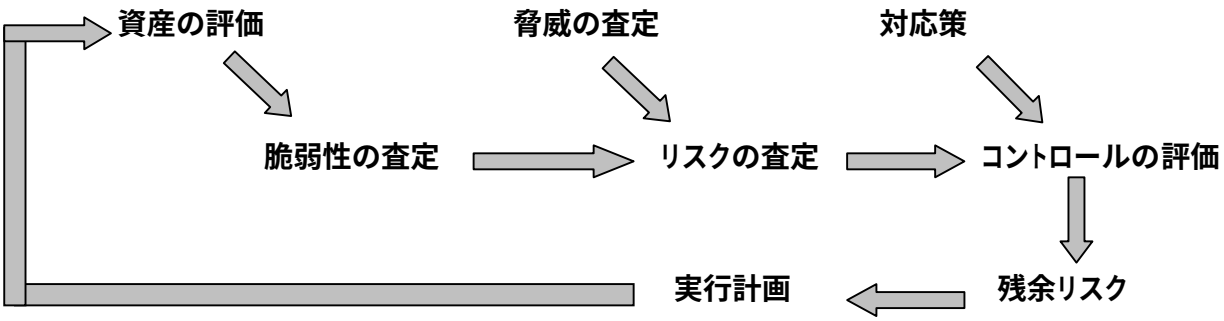
もしビジネス・プロセスがインテグリティの喪失に対して脆弱ならば，特別な対策が取られなければならない。

次に脅威，即ち，何が脆弱性を利用可能かを検討する。その脅威の確率，脆弱性の度合い，影響の重大性，これらが総合的に評価されてリスク査定の結論が出される。その後，対応策（コントロール）を選択し，また有効性を評価する。 さらに残余リスクを明らかにする。

行動計画が作成された後に，サイクルが再び開始可能となる。

† 脆弱性分析の結果が関連する脅威の識別であり，脅威分析によって関連する脆弱性が識別できる

リスク分析のフレームワーク



計画と組織

PO1　戦略的なIT計画の定義

1 組織の長期および短期計画の一部としてのIT
2 ITの長期計画
3 ITの長期計画の策定－方法論と構造
4 ITの長期計画の変更
5 情報サービス機能の短期計画の策定
6 現行システムの評価

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

最高経営責任者
最高業務責任者
最高財務責任者
情報統括役員
情報サービス機能の計画策定／運営委員会メンバ
情報サービス機能の上級管理者，人事サービス・スタッフ

収集すべき証拠資料:

計画策定プロセスに関連する方針と手続き
上級管理者の運営役割と責任
組織の目標と長期/短期計画
情報技術の目標と長期/短期計画
現状レポートと計画策定/運営委員会会議の議事録

コントロール評価

評価視点:

情報サービス機能またはビジネス事業体の方針および手続きが，構造化計画アプローチの使用を指示していること。
方法論は計画の策定と修正に対して適切であり，最低限，以下をカバーしていること。

- 組織の使命と目標
- 組織の使命と目標を支援する情報技術主導
- 情報技術主導に対する機会
- 情報技術主導の実現可能性調査
- 情報技術主導に対するリスク評価
- 現在と将来にわたる情報技術投資対象への最適投資

(評価視点続き)

・組織の使命と目標の変更を反映するための情報技術主導のリエンジニアリング
・データ・アプリケーション，技術および組織に対する戦略の代替案評価

計画策定プロセスの中では，組織変更，技術進化，規制要件，ビジネス・プロセス・リエンジニアリング，スタッフ配置，イン及びアウトソーシング，その他が考慮され，かつ適切に取り扱われていること。

存在する情報技術の長期/短期計画は最新の内容であり，事業体全体，その使命，並びに重要な業務機能を適切に取り扱っていること。

情報技術プロジェクトは，情報技術計画策定に関する方法論の中で明らかにされた適切なドキュメンテイションによって支援されていること。

情報技術の目的と長期および短期計画が，組織の目的と長期および短期計画を満たし続けていることを保証するチェックポイントが存在すること。

情報技術計画に関して，プロセス・オーナと上級管理者によるレビューと承認が行われること。

情報技術計画での現行情報システム評価は，ビジネスの自動化，機能性，安全度，複雑さ，コスト，強みと弱みの程度の観点から行うこと。

► 準拠性テスト:

情報サービス機能の計画/運営委員会会議の議事録は，計画策定プロセスを反映した内容か。

計画策定方法論で示された成果物が存在し，成果物の内容は規程に準拠しているか。

適切な情報技術主導が，情報サービス機能の長期/短期計画に含まれているか。
(即ち，ハードウエア変更，キャパシティ・プランニング，情報アーキテクチャ，新規のシステム開発または調達，災害時回復計画，新しい処理基盤の導入，その他)

情報技術イニシアチブにより，長期および短期計画が支援されているか，また調査，訓練，スタッフ配置，設備，ハードウエア，ソフトウエアに対する要件が考慮されているか。

情報技術主導の技術的な意味が明らかにされているか。

現在と将来への情報技術投資を最適化するための考慮がなされてきたか。

情報技術の長期および短期計画は，組織の長期および短期計画と組織の要求に整合しているか。

計画は，状況の変化に応じて変更されてきたか。

情報技術の長期計画は，定期的に短期計画に変換されているか。

諸計画を実行するタスクが存在するか。

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:

戦略的情報技術計画と，類似した組織または適切な世界標準／業界最良と認識された慣行とのベンチマークの実施

IT主導が，組織の使命と目標を反映している事を保証するために，IT計画の詳細なレビュー組織内の弱みの既知の部分が，情報技術において解決すべき問題として計画され，改善すべきものとして明らかにされているかを見極めるためにIT計画を詳細にレビュー

► 実証性テストの結果:

情報技術による組織の使命と目標の未達成
情報技術による短期計画の長期計画への整合性維持不能
情報技術プロジェクトによる短期計画未達成
情報技術によるコストと納期ガイドライン遵守不能
ビジネス機会の喪失
情報技術機会の喪失

PO2 情報基盤の定義

コントロール目標

1 情報基盤モデル
2 コーポレート･データ･ディクショナリとデータ･シンタックス･ルール
3 データ分類スキーム
4 セキュリティレベル

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報統括役員
情報サービス機能の計画策定／運営委員会メンバ
情報サービス機能の上級管理者
セキュリティ担当役員

収集すべき証拠資料:

情報アーキテクチャに関連する方針と手続き
情報アーキテクチャ･モデル
コーポレート･データ･モデルを含む情報アーキテクチャ･モデルの支援文書
コーポレート･データ･ディクショナリ
データ･オーナシップ方針
上級管理者の運営役割と責任
情報技術の目標と長期および短期計画
状況報告書と計画策定／運営委員会会議の議事録

コントロール評価

評価視点:

情報サービス機能の方針および手続きが，データ･ディクショナリの開発と維持を取り扱っていること。
情報アーキテクチャ･モデルの更新の際に使用されるプロセスは，長期および短期計画に基いており，関連するコストとリスクを考慮しており，モデルへの変更がなされる前に上級管理者の承認が得られることを保証すること。
データ･ディクショナリとデータ･シンタックス･ルールが最新の状態に保持されるようなプロセスが使用されていること。

(評価視点続き)

データ･ディクショナリは，開発場所からアクセスでき，それに対する変更が直ちに反映されることを保証するデータ･ディクショナリ配付手段が使用されていること。
情報サービス機能の方針と手続きによって，セキュリティ分類とデータ･オーナシップを含むデータ分類が取り扱われ，データ･クラスに対するアクセス･ルールが明確かつ適切に定義されていること。
データ分類識別子を有しないデータ資産に関しては，分類に対しデフォルト値が与えられるように標準が定義されていること。
情報サービス機能の方針と手続きが，次に述べることを取り扱っていること。
- ･データ並びにそのデータのセキュリティ属性へのすべてのアクセスに対しては，データ･オーナ（データ･オーナシップ方針に定義されている通り）の承認を必要とする適切な承認プロセスが存在する。
- ･セキュリティ･レベルは，それぞれのデータ分類に対して定義される。
- ･アクセス･レベルが定義されており，それはデータ分類に対して適切である。
- ･機密データへのアクセスには，明示的なアクセス･レベルが必要とされ，データは，「必要最小限の開示」の原則によってのみ提供される。

► 準拠性テスト:

情報アーキテクチャ･モデルの変更は，情報技術の長期/短期計画に対する変更を反映し，また，関連するコストとリスクが明らかにされていることを確認しているか。
データ･ディクショナリへのあらゆる修正と変更による影響を評価し，修正と変更が有効に伝達されていることが保証されるか。
さまざまな稼働中のアプリケーション･システムおよび開発プロジェクトにおいて，データ定義のために，間違いなくデータ･ディクショナリが使用されているか。
データ･ディクショナリの文書化が適切であり，各データ項目毎にデータ属性およびセキュリティ･レベルが定義されていることが確認できるか。
データ分類，セキュリティ･レベル，アクセス･レベル，デフォルトは適切か。
各々のデータ分類が以下を明確に定義しているか。
- ･アクセス権限を持つ者
- ･適切なアクセス･レベルの決定者
- ･アクセスに必要な特別な承認
- ･特殊なアクセス要求（例：非開示，機密合意）

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:

情報アーキテクチャ・モデルと，類似の組織または適切な国際標準／業界最良と認識された慣行とのベンチマークの実施

重要な要素の完全性チェックのために，データ・ディクショナリに対する詳細なレビューの実施

機密データに対して定義されたセキュリティ・レベルを詳細にレビューし，アクセスに対して適切な許可が得られていること，アクセス許可が情報サービス機能の方針と手続きの中で定義されたセキュリティ・レベルと一致していることの立証

► 実証性テストの結果:

情報アーキテクチャ・モデルと次との整合性の欠如:

コーポレート・データ・モデル，コーポレート・データ・ディクショナリ，関連する情報システム，情報技術の長期および短期計画

データ・ディクショナリへの変更の伝達が不十分なことに起因し，適時性を欠き時代後れとなったコーポレート・データ・ディクショナリ項目とデータ・シンタックス・ルール

オーナシップが明確または適切に定義されていないデータ項目

不適切に定義されているデータ・クラス

「必要最小限の開示」規程に準拠していないデータ・セキュリティ・レベル

PO3 技術指針の決定

コントロール目標

1 技術基盤の計画策定
2 将来の動向と規制のモニタリング
3 技術基盤のコンティンジェンシー
4 ハードウェアとソフトウェアの取得計画
5 技術標準

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

最高経営責任者
最高業務責任者
最高財務責任者
情報統括役員
情報サービス機能の計画策定／運営委員会メンバ
情報サービス機能の上級管理者

収集すべき証拠資料:

技術基盤の構築計画と監視に関する方針と手続き
上級管理者の運営の役割と責任
組織の目標と長期/短期計画
情報技術の目標と長期/短期計画
情報技術のハードウエア/ソフトウエア取得計画
技術基盤構築計画
技術標準
現状報告書と計画策定/運営委員会の会議議事録

► 評価視点:

技術基盤計画を策定し，定期的に更新していくためのプロセスが存在すること。 そのプロセスにより，提出された変更について先ず関連したコストとリスクの評価がなされ，計画を変更する前に上級管理者の承認が得られることが確認できること。
技術基盤計画が，情報技術の長期計画および短期計画と比較されていること。
組織の技術面の現状を評価するプロセスが存在し，それはシステム・アーキテクチャ，技術指針，移行戦略といった観点を網羅していることを保証すること。
情報サービス機能の方針と手続きは，現在および将来の技術潮流と規制条件を評価し監視する必要性を取り扱っていること，並びにそれらが技術基盤計画の開発から維持を通して考慮されることを保証すること。
技術の取得に際し，計画のなかで物流および環境面への影響が考慮されていること。
情報サービス機能の方針と手続きによって，コンティンジェンシー対応の技術的計画を系統的に評価する必要性が確実に取り扱われるようになっていること。
(例：構築基盤の冗長性，回復力，適切性と展開能力)
情報サービス機能の管理者が，先端技術を評価し，適切な技術を現在の情報サービス基盤の中に取り入れていること。
ハードウェアとソフトウェアの取得計画は，技術基盤計画内で確認された要件に準拠し，正式に承認されていること。
技術標準は，技術基盤計画に記述された技術上の構成要素に対して適切であること。

準拠性評価

► 準拠性テスト:

情報サービス機能の管理者が，技術基盤計画を理解し利用しているか。
技術基盤計画の変更は，関連するコストとリスクを確認しており，しかもそれらの変更は情報技術の長期/短期計画の変更を反映しているか。
情報サービス機能の管理者が，先端技術を監視，評価し，適切な技術を現在の情報サービス基盤のなかに取り入れるためのプロセスを理解しているか。
情報サービス機能の管理者は，コンティンジェンシー対応の技術計画を系統的に評価するプロセスを理解しているか。(例：構築基盤の冗長性，回復力，適切性と展開能力)
現在導入されているハードウェア/ソフトウェアと現在承認されている取得計画に従って追加される新しいハードウェア/ソフトウェアとを調和させる点に関しては，情報サービス機能の現在の物理的環境は適切か。
ハードウェアとソフトウェアの取得計画は，情報技術の長期/短期計画に準拠し，技術基盤計画の中で明らかにされた要求を反映しているか。
技術基盤計画が，現在並びに将来の技術の利用を取り扱っているか。
技術標準が遵守されていて，開発プロセスの一部として組入れられているか。
アクセス許可は，情報サービス機能の方針および手続きで定義されたセキュリティ・レベルに整合しており，しかも適切なアクセスに対して適切な承認が得られているか。

► 実証性テスト:

技術基盤構築計画と，類似の組織または適切な国際標準／業界最良と認識された慣行とのベンチマーク･テストの実施
重要な要素の完全性チェックのためにデータ･ディクショナリの詳細なレビュー
機密データのために定義されたセキュリティ･レベルの詳細なレビュー

► 実証性テストの結果:

情報アーキテクチャ･モデルと次との整合性の欠如
コーポレート･データ･モデル，コーポレート･データ･ディクショナリ，関連する情報システム，情報技術の長期/短期計画
時代後れのコーポレート･データ･ディクショナリ項目とデータ･シンタックス･ルール
技術基盤計画で取り扱われていないコンティンジェンシー対応
技術基盤計画の要件を反映していない情報技術ハードウェア/ソフトウェアの取得計画
技術基盤計画または情報技術ハードウェア/ソフトウェアの取得計画に一致しない技術標準
技術標準と整合しない技術基盤計画または情報技術ハードウェア/ソフトウェアの取得計画
データ･ディクショナリに記述されていない重要な要素
然るべく分類されていない，またはセキュリティ･レベルを持たない機密データ

PO4　IT組織と関連の定義

コントロール目標

1 情報サービス機能の計画策定あるいは運営委員会
2 情報サービス機能の組織的な配置
3 組織的達成のレビュー
4 役割と責任
5 品質保証の責任
6 論理的および物理的セキュリティの責任
7 オーナシップとカスタディアンシップ
8 データとシステムのオーナシップ
9 監督
10 職務の分離
11 IT要員の配置
12 情報サービス機能の要員に関する職務あるいは職位記述
13 重要なIT要員
14 契約要員の手続
15 諸関連

高レベルかつ詳細なコントロール目標の監査手続

理解

► **面接対象者**:

最高経営責任者
最高業務責任者
最高財務責任者
情報統括役員
品質保証担当役員
情報セキュリティ担当役員
情報サービス機能の計画策定/運営委員会メンバ, 人事, 上級管理者

► **収集すべき証拠資料**:

上級管理者の計画策定/運営の役割と責任
組織の目標と長期/短期計画
情報技術の目標と長期/短期計画
情報サービス機能と他の機能との関係を示す組織図
IT組織と諸関連に関する方針と手続き
品質保証に関する方針と手続き
情報サービス機能の要員配置要求を決定するのに使われる方針と手続き
情報サービス機能の組織図
情報サービス機能の役割と責任
情報サービス機能の要職についての職位 (職務) 記述書
状況報告書と計画策定／運営委員会会議の議事録

コントロール評価

► 評価視点:

経営方針書と上級管理者の方針の伝達により，情報サービス機能の独立性と権限が保証されていること。

情報サービス機能の計画策定／運営委員会の地位と機能が定義されていて，責任が明確になっていること。

情報サービス機能の計画策定／運営委員会の規程によって，委員会のゴールが，組織の目標および長期/短期計画，情報技術の目標および長期/短期計画に沿ったものとなっていること。

情報管理上の問題を明らかにし解決するために適切なプロセスが存在し，意識が喚起され，理解およびスキルの向上が図られていること。

方針書によって，目標や環境の変化に適合させるために，組織構造を評価し修正する必要性が示されていること。

情報サービス機能の有効性と受諾を判定するプロセスと業績指標が存在すること。

上級管理者が役割と責任の遂行を保証していること。

情報システム，内部統制およびセキュリティに関して，組織内全員の役割と責任についての要点を示した方針が存在すること。

内部統制とセキュリティに関し意識と規律の向上が図れるような定期的かつ組織的な運動が存在すること。

品質保証に関する機能と方針が存在すること。

品質保証機能は，システム開発要員からは十分な独立性を保持していること。 また，その責任を全うするために適切な要員の配置が行なわれ，要員は十分なる専門的知識を有すること。

資源を計画し，品質保証テストの完了を保証し，システムの構築または変更についての実施前の承認を保証する適切な品質保証プロセスが存在すること。

経営者が，情報セキュリティ担当役員に対して，内部統制とセキュリティ（論理的かつ物理的セキュリティの双方）の方針と手続きの公式化に関する組織的責任を正式に与えていること。

情報セキュリティ担当役員は，その役割と責任が組織の情報セキュリティ方針に一致したものであることを十分に理解し明らかにしていること。

組織のセキュリティ方針は，それぞれの情報資産オーナ（例:ユーザ，管理者，セキュリティ担当者）が実施すべき情報セキュリティに対する責任を明確に定義していること。

すべての主要なデータ資源とシステムに対して，データとシステムのオーナシップを網羅する方針と手続きが存在すること。

データおよびシステムのオーナシップの変更を定期的にレビューし維持していくための手続きが存在すること。

役割と責任が正しく行使され，すべての人が役割と責任を遂行するに充分な権限と資源を有することを保証する監督実務に関する方針と手続きが存在すること

職務の分離は，次の二者間に存在すること。

- ･システムの開発と保守
- ･システムの開発とオペレーション
- ･システムの開発／保守と情報セキュリティ
- ･オペレーションとデータ管理
- ･オペレーションとユーザ
- ･オペレーションと情報セキュリティ

(評価視点続き)

効果的な技術的ソリューションを提供できることを保証するために，情報サービス機能のスタッフが配置され能力が維持されていること。
情報サービス機能の職位（職務）記述書を評価し再評価するための方針と手続きが存在すること。
システム開発ライフサイクル活動（要件定義，設計，開発，テスト），情報セキュリティ，取得およびキャパシティ・プランニングを含む重要なプロセスに対しては，適切な役割と責任が存在すること。
適切で有効な重要業績指標および/または重要成功要因が，組織目標達成のために情報サービス機能の業績を測定する際に利用されていること。
情報サービス機能の方針と手続きによって，コンサルタントおよび他の契約社員の活動が管理されており，それにより組織の資産の保護が保証されていること。
情報技術サービス契約の手続が適切であり，組織の取得方針に一致したものとなっていること。
情報サービス機能役員の内外双方の利害関係が調整され，意思疎通が計られ文書で裏付けられるプロセスが存在すること。

► 準拠性テスト:

情報サービス機能の計画策定/運営委員会は，情報サービス機能とその活動を監督し活動項目を決定しているか。
情報サービス機能に関して，報告の階層構造は適切であるか。
最高経営管理者との協力関係を維持する上で，組織内における情報サービス機能の位置づけは効果的か。
情報サービス機能の上級管理者は，情報サービス機能の業績を監視し評価し報告するために，どのようなプロセスが使用されているかを理解しているか。
重要な指標が，業績の評価に用いられているか。
実績が目標レベルに達していない時に取るべき是正措置を決定するために，達成目標に対し実績を分析するプロセスが存在するか。
予想された業績レベルから著しく乖離した時に，管理者によって対応策が施されたか。
ユーザ/オーナの管理者は，ユーザ/オーナのニーズに合った情報技術解決策を提供する情報サービス機能の対応と能力を評価しているか。
情報サービス機能の管理者は，その役割と責任を自覚しているか。
テスト並びに情報サービス機能のプロジェクト計画承認に品質保証部門が関与しているか。
情報セキュリティ要員は，核となるオペレーティング・システムとアプリケーション・システムをレビューしているか。
情報セキュリティ機能による現状のまたは開発中の情報セキュリティ（論理的，物理的共に）評価報告書/文書は適切であるか。
情報セキュリティの方針と手続きに対する自覚は十分か，また，その適用に矛盾はないか。
要員は情報セキュリティと内部統制の研修に出席しているか。
すべての情報資産に対して，データおよびシステムに関するオーナシップが定義されているか。
データおよびシステムの変更は，データおよびシステムのオーナにより承認されてきたか。
すべてのデータおよびシステムに対して，それらの管理レベルに責任を持つオーナまたは管理者がいるか。

(準拠性テスト続き)

すべてのデータおよびシステム資産へのアクセスが，その資産のオーナによって承認されているか。
職位（職務）上の権限と監督の関係は，在職者の責任と釣り合いがとれているか。
職位（職務）記述書は，権限と責任の双方について明確に記述しているか。
職位（職務）記述書は，必要とするビジネス，関連する/技術的な能力を明確に記述しているか。
職位（職務）記述書は，正確に伝達され，個々人によって理解されているか。
情報サービス機能関連の職位（職務）記述書には，要員に伝達されてきた重要な業績指標が含まれているか。
情報サービス機能スタッフの職務と責任が，公表された職位（職務）記述書と組織図に一致しているか。
職位（職務）記述書が，重要な職位に対して適切であり，そのなかに情報システム，内部統制とセキュリティに関する組織からの委任が含まれているか。
職位（職務）記述書は，その職位についている在職者の職責と比較して見て，正確に記述されているか。
意図した職務の分離および情報サービス機能内の機能の限定に対する準拠性の性質と程度は適切か。
情報技術スタッフの配置により能力は維持されているか。
責任，権限および業績基準を適切かつ明確に示すための根拠として，職位（職務）記述書は適切か。
契約管理責任が適切な要員に割り当てられているか。
契約の条項は，契約のための通常の組織標準に一致しているか。また，標準的な契約の条件と条項が弁護士によりレビューされ評価され同意されているか。
契約に，コーポレート・セキュリティ，内部統制方針，情報技術標準の厳守に関する適切な条項が含まれているか。
プロセスおよび/または構造によって，良い関係を維持する為に必要な有効かつ効率的な調整が規定されているか。

► 実証性テスト:

組織と諸々の関係に対して，類似した組織または適切な国際標準/業界最良と認識された慣行とのベンチマークを実施する。
効果的でない情報サービス機能の計画策定/運営委員会が，組織にどのような影響を与えているかを確認するために詳細なレビューを実施する。
情報システムの諸問題に対処しながら技術的解決を提供している情報サービス機能の進捗度を見るために詳細なレビューを実施する。
組織構造，スタッフ配置と要員の能力，割当てられた役割と責任，データとシステムのオーナシップ，監督，職務の分離等を評価する詳細なレビューを実施する。
品質保証機能に対し詳細なレビューを実施し，組織の要求を満たす上での有効性を判定する。
情報セキュリティ機能に対し詳細なレビューを実施し，組織全体のセキュリティ（論理的および物理的共に）およびセキュリティ意識教育の提供に関してその有効性を判定する。
契約をサンプリングして詳細なレビューを実施し，契約が両者間で正しく実行されていて，組織の標準的

(実証性テスト続き)

な契約条件に準拠していることを確認する。

► 実証性テストの結果:

情報サービス機能計画策定／運営委員会による監督が効果的でないために情報サービス機能とその活動に弱みが生じている。

組織構造のギャップ，オーバーラップ等の存在が，情報サービス機能に有効でなくまたは効率的でないものをもたらしている。

不適切な組織構造，欠けている機能，不十分なスタッフ配置，能力不足，不適切な役割と責任，データ並びにシステムのオーナシップの混乱，監督上の問題，職務分離の欠如等の存在。

品質保証要求を満たさないで，開発され，修正され，提供されてきたシステムの存在。

セキュリティ要件（論理的か物理的の一方または両方）を満たさないで開発され，修正され，提供されてきたシステムの存在。

組織の契約要件を満たさない契約の存在。

情報サービス機能と，情報サービス機能内外の利害関係者間で非効果的な調整と意志疎通が計られてきた。

PO5 IT投資の管理

コントロール目標

1 情報サービス機能の年次運営予算
2 コストと便益のモニタリング
3 コストと便益の正当化

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

最高財務責任者
情報統括役員
情報サービス機能の計画策定/運営委員会メンバ
情報サービス機能の上級管理者

収集すべき証拠資料:

予算とコストに関する組織の方針，方法および手続き
予算とコストに関する情報サービス機能の方針と手続き
情報サービス機能の現在および前期の年次運営予算
組織の目標と長期/短期計画
情報技術の目標と長期/短期計画
上級管理者の計画策定/運営の役割と責任
意見の差異の監視と管理に関係した差異レポートおよびその他の伝達
状況レポートと計画策定/運営委員会の会議議事録

コントロール評価

評価視点:

情報サービス機能の予算作成プロセスが，組織のプロセスと整合していること。
組織の予算と長期/短期計画，並びに情報技術の長期/短期計画に整合する情報サービス機能の年次運営予算が作成され，適切に承認されることを保証する方針と手続きが存在すること。
予算作成プロセスには，情報サービス機能の予算作成に貢献している情報サービス機能の主要な部署の管理者が参画していること。
実際のコストを定期的に監視し，それらを予測コストと比較する適切な方針と手続きが存在し，実際のコストは組織の原価計算制度に基づいていること。
適切な方針と手続きによって，情報サービス機能によるサービス提供がコスト面から正当化され，事業コストの範囲内に有るように保証されていること。

準拠性評価

► 準拠性テスト:

情報サービス機能に対する財政的援助は，情報サービス機能の年次運営計画を正当化する上で適切か。
情報サービス機能のコストの種類が，分かり易く適切に正しく分類されているか。
情報サービス機能の活動に関連したコストを，日常的に記録し，処理し，報告する為のシステムは適切か。
コスト監視プロセスによって，予算と実績が適切に比較されているか。
影響を受けるユーザ･グループの管理者，情報サービス機能および組織の上級管理者によるコスト効果分析は適切にレビューされているか。
コスト監視に利用されるツールが，有効でありかつ正しく利用されているか。

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:

予算とコストに関して，類似の組織または適切な国際標準/業界最良と認められた慣行とのベンチマークを実施する。
前年と当年の予算と実績，その差異，並びに取られた是正処置に対して詳細なレビューを実施する。

► 実証性テストの結果:

組織の予算と長期/短期計画，並びに情報技術の長期/短期計画に従っていない情報サービス機能予算の存在。
把握されていない情報サービス機能の実コストの存在。

PO6 マネジメント目標と指針の伝達

コントロール目標
1 積極的な情報のコントロール環境
2 方針に対する経営者の責任
3 組織方針の伝達
4 方針実施の資源
5 方針の保守
6 方針，手続および標準への準拠
7 品質の協定
8 セキュリティおよび内部統制フレームワークの方針
9 知的財産権
10 特定課題の方針
11 ITセキュリティ意識の伝達

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

最高経営責任者
最高業務責任者
最高財務責任者
情報統括役員
セキュリティ担当役員
情報サービス機能の上級管理者
情報サービス機能の計画策定/運営委員会メンバ

収集すべき証拠資料:

以下に関する方針と手続き:
管理者の積極的なコントロール･フレームワークと意識喚起プログラム，セキュリティと内部統制フレームワーク，情報サービス機能の品質プログラム
上級管理者の運営任務と責任
組織の目標と長期/短期計画
情報技術の目標と長期/短期計画
状況報告書と計画策定/運営委員会の会議議事録
意志疎通プログラム

評価視点:

組織の方針と手続きにより，フレームワークと意識喚起プログラムが作成され，情報技術に対し特別な注意が向けられ，積極的なコントロール環境が促進され，以下が取り扱われていること。

- インテグリティ
- 倫理的価値観
- 行動規範
- セキュリティと内部統制
- 個人の能力
- 経営者の哲学と運営スタイル
- 重役会またはそれと同等の委員会により規定される会計責任，注意および指示

最高経営管理者が模範を示して，積極的なコントロール環境を促進していること。

管理者が，全般的な目標と指針を管理する方針についてその公式化，作成，文書化，公表，コントロール，定期的なレビューを実施する全責任を負っていることを認めていること。

正式な意識喚起プログラムの存在によって，経営者の積極的なコントロール環境に関して継続的な意志疎通が図られ研修が提供されること。

組織の方針をタイムリーに実施するために，適切で充分な資源があてがわれることを保証する組織の方針と手続きが存在すること。

適切な手続きによって，個人が導入された方針と手続きを理解し，その方針と手続きが遵守されるようになっていることを保証できること。

提供されるシステムとサービスの品質を左右する哲学，方針，目標が，情報サービス機能の方針と手続きにより正式に定義され，文書化され，維持されていること。　また，その哲学，方針，目標は，組織のそれらと整合性を有すること。

情報サービス機能の管理者は，品質に関する哲学，方針および目標が，情報サービス機能のあらゆるレベルで理解され，実施され，維持されていることを保証すること。

情報技術に関連する重要な標準，指針，方針と手続きが定期的にレビューされ，再認可される必要があることを管理する手続きが存在すること。

上級管理者は，セキュリティと内部統制への全体的なアプローチのためのフレームワーク開発に対し全責任を取り続けていること。

セキュリティと内部統制フレームワーク文書は，以下につき明確に記すこと：

セキュリティと内部統制に関する方針，効果と目的，管理構造，組織内の範囲，責任の分担，セキュリティと内部統制方針を遵守しなかった場合の罰則と懲戒処分の定義

正式なセキュリティと内部統制の方針は，組織の内部統制プロセスを明らかにし，以下のコントロールの構成要素を含むこと：

- コントロール環境
- リスク評価
- コントロール活動
- 情報と伝達
- 監視

特別な活動，アプリケーション，システムまたは技術に関する管理者の決定については，その文書化を要求する明確な方針が存在すること。

► 準拠性テスト:

積極的なコントロールの促進に向けられている管理者の努力は，重要な側面（例えば，インテグリティ，倫理観，行動規範，セキュリティと内部統制，個人の能力，経営の哲学と運営スタイル，会計責任，注意，与えられた指針）を網羅しているか。
従業員は，行動規範を受け入れ，それを理解しているか。
管理者は，組織の内部統制環境を取り扱っている方針を伝達しているか。
管理者は，内部統制環境を網羅する方針を公式化，開発，文書化，普及，管理するために，資源の提供を約束しているか。
管理者は，状況の変化に適応するために標準， 指針，方針と手続きを定期的にレビューし，適切性並びに能力の継続的保持に勉めているか。
管理者の監視努力は，組織の諸方針を適時に導入するために，適切かつ充分な資源が調達されていることを保証しているか。
内部統制環境についての標準，指針，方針，手続きに関連する管理者の実施努力は，全組織を通して準拠性を保証しているか。
品質に関する哲学，方針，目標は，組織と情報サービス機能の哲学，方針，手続きに準拠し整合性を有しているか。
情報サービス機能の管理者，開発と運用スタッフを抽出調査し，品質の哲学と関連する方針，手続き，並びに目標が，情報サービス機能のすべてのレベルで理解され遵守されているかを評価する。
品質測定プロセスは，組織目標の達成を保証しているか。
管理者を抽出し，彼等が自己のレビュー責任下にあるセキュリティおよび内部統制活動（例えば，例外レポート，照合調整，比較）に関わっており，その内容を理解しているかを評価する。
個々人の役割，責任，権限は，組織のすべてのレベルで明確に伝達され理解されているか。
部門を抽出し，セキュリティと内部統制活動を日常的に監視する手続き（例えば，例外レポート，照合調整，比較）を評価し，経営管理者にフィードバックするプロセスが遵守されているかを評価する。
システム文書を抽出し，システム特有の問題に対する管理者の決定が文書化され，組織の方針と手続きに準拠して承認されているかを評価する。
システム文書を抽出し，特別な活動，アプリケーション・システムまたは技術に関わる管理者の決定が確実に上級管理者によって承認されているかを確認する。

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:

管理者の情報コントロール・フレームワーク並びに意識喚起プログラムと，類似した組織または適切な国際標準／業界最良と認められた慣行とのベンチマークを実施する。
プロジェクトが，リスクとコスト対効果の分析に基づいて優先順位づけされ承認されているかを判定するために，承認されたセキュリティと内部統制関連のプロジェクトをサンプリングして詳細なレビューを実施する。

► 実証性テストの結果:

組織全体にわたり建設的な内部統制環境を促進している管理者の公約に疑問をもたらすコントロール・フレームワーク弱点の存在。
組織の内部統制環境を取り扱っている方針の伝達に関する管理者の不履行。
内部統制環境を網羅する方針の公式化，作成，文書化，普及，管理のために手当てされるべき資源の不足。
最新でない標準，指針，方針，および手続き。
管理者による準拠性監視が不適切なために，標準，指針，方針と手続きが組織全体を通して遵守されていることの保証不可。
品質に関する哲学，方針と目標を効果的に定義，文書化，維持，伝達するのに必要な情報サービス機能の質と能力に関する公約上の諸欠陥。
組織並びに情報サービス機能のセキュリティと内部統制フレームワークに存在する弱点。
特別な活動，アプリケーションまたは技術を取り扱う上で必要な特定方針の布告の欠落。

PO7 人的資源の管理

コントロール目標
1 要員の採用と昇進 2 要員の資格 3 要員の教育 4 相互教育あるいは代替要員 5 要員の身元調査手続 6 従業員の業績評価 7 職務の交替および終了

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

人事の担当役員および選定された要員
セキュリティ担当役員
選定されたセキュリティ担当要員
情報サービス機能管理者
情報サービス機能人事担当役員
選定された情報サービス機能管理者
選定された情報サービス機能の要員
情報サービス機能内の機密に関わる職務にある選定された要員

収集すべき証拠資料:

人的資源の管理に関する方針と手続き
職位記述書，業績評価フォーム，訓練と育成フォーム
選定された職位と要員に関する要員ファイル

コントロール評価

評価視点:

空席補充のための要員採用と選抜に関して基準が用いられていること。
適切ならば，職業専門家組織に対する適切な要件を考慮して，スタッフ職務に要求される資質が明細に記述されていること。
管理者と従業員が，職務適性プロセスについて応諾していること。
訓練プログラムは，情報セキュリティの問題を網羅する教育並びに一般的な意識に関しては，文書で示された組織の最低限の要求と整合性を有すること。
管理者が，要員教育とキャリア開発を公約していること。

(評価視点続き)

技術上の並びに管理上のスキル･ギャップが明らかにされ，それらのギャップに対処するために，適切な対策が取られていること。
重要な職務機能に関しては，継続した相互教育と要員のバックアップがなされていること。
中断されない休暇取得の強制が実施されていること。
組織の機密事項取り扱い許可手続きが適切であること。
従業員は，その職位に関する標準的な能力プロフィールに基づいて評価され，評価は定期的に実施されていること。
職務の交替と終了のプロセスは，組織の資源保護を保証すること。
人的資源管理の方針と手続きは，適用される法律と規制に準拠したものであること。

► 準拠性テスト:

採用，昇進，選抜の基準は，その職位の要求に対して客観的かつ適切であるか。
要員は，その職務機能の遂行，又は責任範囲に関し適切な知識を持っているか。
現存する職位（職務）記述書はレビューされ，最新の状態に更新されているか。
人事ファイルの内容には，組織全体の教育および一般的な意識喚起プログラムに対する要員の理解について当人の承認データが含まれているか。
重要な職に携わる適切な要員のために，継続的な訓練および教育が行われているか。
情報セキュリティ要員は，セキュリティに関する手続きと技術について適切な訓練を受けているか。
情報サービス機能の管理者とスタッフは，組織の方針および手続きを知っており，かつ理解しているか。
機密事項取り扱い許可の調査プロセスは，適用されるプライバシー統制法規に従っているか。
重要な情報サービス機能に携わる要員は，ビジネス目標に関する知識として，内部統制の哲学，情報システムのセキュリティと統制概念を理解しているか。

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:

人的資源の管理活動と，類似した組織または適切な国際標準/業界最良と認められた慣行との間でベンチマークを実施する。
情報サービス機能の人的資源管理活動について詳細なレビューを実施する。

► 実証性テストの結果:

その仕事につく可能性があるかまたは実際の候補者から反対/不満がある。
採用，異動，昇進，退職について，以下に示す矛盾が存在する:
- 遵守されない方針，手続き

(実証性テストの結果続き)

・適切な管理者により承認されていない行為
・職務規程および要員の資格に基づいていない行為

要員について:

・資格が不適当である
・能力の相違を考慮した訓練および育成の機会が与えられていない
・業績評価は，実施されていないか，又は当人の職位/実施中の仕事が考慮されていない
・雇用の際に，セキュリティ調査が実施されていない
・セキュリティ調査が定期的に実施されていない

訓練計画と要員育成活動が不適切である。
重要な要員の相互訓練とバックアップが不適切である。
承認されていないセキュリティ方針を容認している。
訓練し要員を育成するための予算と時間が不適切である。
重要な職務を遂行している要員の勤務報告書が，休日勤務および休暇未取得の状況を示している。

PO8 外部要件への準拠性の保証

コントロール目標

1 外部要件のレビュー
2 外部要件に準拠するための実務と手続
3 安全と人間工学への準拠
4 プライバシー，知的財産権とデータフロー
5 電子商取引
6 保険契約への準拠

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

顧問弁護士
人事担当役員
情報サービス機能の上級管理者

収集すべき証拠資料:

次の諸問題に関連する政府または外部の要件（例：法律，法令，ガイドライン，規制と標準）：
対外関係と外部要件のレビュー，安全性と保険衛生（人間工学を含む）への準拠性の問題，プライバシーの問題，情報システムのセキュリティ要件，暗号化データの送信（国内および国際間の両方）
電子商取引の使用に関しての国家的および/または国際的な“会計基準/意見表明”
電子商取引の使用に関連する課税裁定
以下に関する標準，方針，手続き
- 外部要件のレビュー
- 安全性および健康衛生（人間工学を含む）
- プライバシー
- セキュリティ
- 入力，処理，蓄積，出力，および送信されるデータの機密性の程度
- 電子商取引
- 保険

適用可能範囲での，すべての電子取引相手先および電子データ交換（EDI）ベンダとのすべての契約書のコピー
情報サービス機能に関連する保険契約書のすべてのコピー
保険契約のUberrimae Fidei(“最も完全なる信義”)要求に対する顧問弁護士の助言
（“最も完全なる信義”は，被害者と加害者の双方に，リスクに対して重要なすべての問題をお互いにすべて公開することを要求する。 もし，こうした良い関係が示されない場合は，その契約は被害者にとって無効であり，また，加害者はその契約を強制できない）
外部監査人，第三者機関のサービス・プロバイダおよび政府諸官庁からの監査報告書

評価視点:

方針と手続きが以下に対して適切であること。

- ･外部要件レビューに関連して適切な是正措置が適時に取られ，かつ継続的な準拠性を保証する適切な手続きが存在することを保証する
- ･外部要件への準拠性を保証する是正措置が適時に取られることを保証するために，外部要件レビューを調整する
- ･適切な防護対策，安全性，並びに保険衛生の各目標への対応
- ･適切な安全性と保険衛生のための訓練と教育が，全従業員に提供されていることの保証
- ･適用される安全性と保険衛生に関する法律と規制への準拠性の監視
- ･プライバシーに関し適切な指針/焦点を持つことにより，すべての法的要件がその範囲内に入るようにする
- ･情報サービス機能環境に対する重要な変更はすべて保険業者へ通知
- ･保険契約要件への準拠性の保証
- ･新規/修正の保険契約が，契約時に更新されることの保証

セキュリティ上の手続きが，すべての法的要件を遵守し，適切に取り扱われていて，以下を含むこと。

- ･パスワードの保護とソフトウェアによるアクセス制限
- ･権限付与手続き
- ･端末に対するセキュリティ対策
- ･データ暗号化対策
- ･ファイアウォール管理
- ･ウィルスからの保護
- ･違反報告書に対する適時なフォローアップ

準拠性評価

準拠性テスト:

外部要件のレビューは次の通りであるか。

- ･法律，行政および規制の問題に関して，最新にして，完全かつ包括的な内容である
- ･手際よい是正措置が取られている

情報サービス機能内の安全性および保健衛生のレビューによって，外部要件への準拠性が保証されているか。

安全性および保険衛生標準に準拠していない問題領域は改正されているか。

情報サービス機能は，文書化されたプライバシーとセキュリティに関する方針および手続きに準拠しているか。

国境を越えて伝送されるデータは，輸出規制に違反していないか。

電子商取引の取引先との契約は，組織の方針および手続きで示された要件を適切に取り扱っているか。

現行の保険契約は，組織の方針および手続きで示された要件を適切に取り扱っているか。

(準拠性テスト続き)

使用される暗号のタイプに規程制限が課せられている場合（例：キーの長さ），使用しようとしている暗号は，その規制に準拠しているか。
規程または内部手続きによって，あるデータ項目が高度な保護および/または暗号化が必要とされている場合（例：銀行でのPIN番号，税金のファイル番号，パスワード，軍事情報），そのようなデータに対し，必要な保護/暗号が施されているか。
組織により展開中の現在のEDIプロセスは，組織の方針および手続きへの準拠性，個々の電子商取引取引先との契約（適用可能なら，EDIベンダとの契約書）への準拠性を保証しているか。

► 実証性テスト:

外部要件への準拠性，ＥＤＩ事業，並びに保険契約要件と，類似した組織または適切な世界標準/業界最良と認められた慣行とのベンチマークを実施する。
是正措置が取られてきたかまたは取られている最中であることを保証するために，外部要件レビュー・ファイルに対して詳細なレビューを実施する。
機密の/プライベートな情報（内部手続きまたは外部規制の何れかにより定義される）に適切なセキュリティおよびプライバシー保護が与えられるているかを評価するために，セキュリティ報告書の詳細なレビューを実施する。

► 実証性テストの結果:

組織において，遵守されていない外部要件の存在。
外部要件レビューの結果，未解決/未訂正のままである重要な活動の存在。
作業環境に関して，対応されていない安全性および保健衛生（人間工学を含む）リスクの存在。
データ・フローおよび/または国境を越えるデータ・フローに関して，プライバシーおよびセキュリティ上の弱点の存在。
電子商取引の故障。
通信プロセス，取引メッセージ，セキュリティ，データ保管に関し，取引先との契約に存在する弱点
取引先との信頼関係に存在する弱点。
保険填補に関する弱点/失効。
保険契約条件に準拠していないものの存在。

PO9 リスク評価

コントロール目標
1 ビジネスリスクの評価 2 リスク評価方法論 3 リスクの識別 4 リスクの測定 5 リスクの行動計画 6 リスクの受容

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報サービス機能の上級管理者
抽出された情報サービス機能要員
抽出されたリスク管理要員

収集すべき証拠資料:

リスク評価に関する方針と手続き
ビジネス･リスク評価文書
経営リスク評価文書
情報サービス機能のリスク評価文書
リスクおよびリスクのエクスポージャーを推定するための根拠の詳細
抽出されたリスク評価要員に関する要員ファイル
残余リスクをカバーする保険証券

コントロール評価

評価視点:

体系的なリスク評価フレームワークは，適切であり，組織目標の達成に関連した情報リスクを含み，リスクが受容可能なレベルにまでどのように管理されるべきかを決定するための基礎を成していること。
リスク評価方法は，全体的および特定システムの双方のレベルで，リスク評価の定期的な更新を規定すること
リスク評価手続きは適切であり，識別されたリスクが外部と内部の双方の要因を含むことを決定でき，監査/検査/識別された発生事象の結果を考慮していること。

(評価視点続き)

組織的目標がリスク識別プロセスに含まれていること。
システム処理活動内の変化を監視する手続きに依って，システムのリスクとエクスポージャーがタイムリーに調整されているかが判別できること。
リスク評価を継続的に監視し改善する手続き，並びにコントロールを創り出すプロセスを削減する手続きが存在すること。
リスク評価文書には，以下が含まれていること。
- ･リスク評価方法論の記述
- ･重要なエクスポージャーと対応するリスクの識別
- ･リスクと対応するエクスポージャー

確率，頻度および脅威の分析技術がリスクの識別に含まれていること。
リスク評価要員の資格が適切であること。
リスク，脅威，エクスポージャーの識別と推定のために，正式な定量的または定性的（あるいは双方の組合せ）な方法が存在すること。
リスク，脅威およびエクスポージャーの推定に，計算並びにその他の方法が用いられていること。
リスク行動計画が，リスク，脅威およびエクスポージャーを軽減する適切な対策として使用されていること。
残余リスクの受容は次を考慮すること。
- ･組織の方針
- ･リスクの識別と推定
- ･リスク評価方法そのものに含まれる不確実性
- ･安全保護およびコントロールを導入する際のコストと効果

保険填補により残余リスクを補うこと

► 準拠性テスト:

リスク評価フレームワークに関しては，リスクを受容可能なレベルにまで減少させるために，リスク評価が定期的に更新されなければならないが，それは遵守されているか。
リスク評価文書は，リスク評価フレームワークに準拠しているか，また，文書は適切に用意され，維持されているか。
情報サービス機能の管理者と要員は，リスク評価プロセスを知っており，それに関与しているか。
管理者は，リスク関連要因と脅威の可能性を理解しているか。
関係する要員は，残余リスクを理解し，正式に容認しているか。
明らかにされたリスクをレビューし同意を得るために，また，リスク減少活動の監視に利用してもらうために，上級管理者への報告書の提出は，タイムリーに行われているか。
リスク分析方法は，リスクのエクスポージャーを定量的または定性的（あるいは双方の組合せ）測定値に依って捉えているか。
管理者によって明らかにされるリスク，脅威，エクスポージャー，並びにリスク関連特性は，特定された脅威の発生を発見するのに利用されているか。
リスク行動計画は最新のものであり，リスク･エクスポージャーを軽減させるためのコントロールとセキュリティ対策はコスト対効果が良いか。

(準拠性テスト続き)

優先順位が最高から最低へと付けられており，各々のリスクに対して適切な対応が取られているか：
- ・計画的な予防手段による減少管理
- ・2番めとして，発見的コントロール
- ・3番めとして，修正的コントロール

‘リスク’対‘管理’のシナリオが文書化され，最新の内容であり，適切な要員に伝達されているか。

容認された残余リスクに関して保険の填補は充分であり，以下の如き様々な脅威のシナリオに対する考慮がなされているか。
- ・火災，洪水，地震，竜巻，テロリズム，その他の予期できない自然災害
- ・従業員の受託責任不履行
- ・ビジネスの中断－収入の枯渇，顧客の喪失，その他
- ・上記の通り，情報技術，ビジネスリスク，ビジネス継続性計画によっては，通常カバーされないその他のリスク

► 実証性テスト:

リスク評価フレームワークに関して，類似の組織または適切な世界標準／業界最良と認められた慣行とのベンチマークを実施する。

リスクを識別し，推定し，残余リスクを容認できるレベルにまで減少させるために使用されるリスク評価方法の詳細なレビューを実施する。

► 実証性テストの結果:

明らかにされていないリスクの存在。

測定されていないリスクの存在。

容認できるレベルにまで対応/管理されていないリスク。

最新でないリスク評価および/またはリスク評価のなかに最新でない情報の存在。

リスク，脅威およびエクスポージャーに関して，誤った定量的/定性的な尺度の存在。

コスト対効果の良い管理やセキュリティ対策を規定していないリスク行動計画。

公式に容認されていない残余リスクの存在。

不適切な保険填補。

PO10 プロジェクト管理

コントロール目標
1 プロジェクト管理のフレームワーク
2 プロジェクト開始におけるユーザ部門の参画
3 プロジェクトチームメンバと責任
4 プロジェクトの定義
5 プロジェクトの承認
6 プロジェクトフェーズの承認
7 プロジェクトマスタ計画
8 システムの品質保証計画
9 保証方法の計画策定
10 正式なプロジェクト･リスク管理
11 テスト計画
12 教育計画
13 導入後レビュー計画

高いレベルと詳細コントロール目標の監査手続

理解

面接対象者:

品質管理者
プロジェクトの品質管理者／コーディネーター
プロジェクト･オーナ／スポンサー
プロジェクト･チーム･リーダ
品質保証コーディネーター
セキュリティ担当役員
情報システム機能の計画策定／運営委員会メンバ
情報システム機能の管理者

収集すべき証拠資料:

プロジェクト管理フレームワークに関する方針と手続き
プロジェクト管理方法論に関する方針と手続き
品質保証計画に関する方針と手続き
品質保証方法に関する方針と手続き
ソフトウェア･プロジェクト･マスタ･プラン（ SPMP）
ソフトウェア品質保証計画（SQAP）
プロジェクト進捗報告書
進捗報告書と計画策定／運営委員会の会議議事録
プロジェクト品質報告書

評価視点:

プロジェクト管理フレームワークは以下を満たしていること:

- プロジェクトを管理するために範囲と境界を定義している。
- 承認されている業務計画とこの計画に従って優先順位づけされた諸プロジェクトとの整合性をレビューするためのプロジェクト要求を規定している。
- 着手される各プロジェクトで採用され，また適用されるプロジェクト管理方法論が定義され，それには以下が含まれる。
- プロジェクト計画
- 要員配置
- 責任と権限の割り当て
- タスク分割
- 時間と資源に関する予算計上
- マイルストーン
- チェックポイント
- 承認
- 完全であり，最新である。
- 開発，導入，改訂プロジェクトを定義し承認する際に，影響を受けるユーザ部門（オーナ/スポンサー）管理者の参加を規定している。
- スタッフ・メンバのプロジェクトへの任命基準を明記している。
- プロジェクト・チーム・メンバの責任と権限を定めている。
- プロジェクトの作業開始前に，プロジェクトの性質と範囲を定義した明確な文書の作成を規定している。
- プロジェクトの性質と範囲を明確に記述した初期プロジェクト定義文書を規定している。
- プロジェクトに着手する以下の理由を含む。
    - 矯正すべき問題，あるいは改善すべきプロセスについての記述
    - 目標達成のために，当該プロジェクトに対して組織能力を高める必要性を示した記述
    - 関連する既存システムの欠陥についての分析
    - 運用の経済性や効率性を増すために与えられる機会
    - プロジェクトで履行されるであろう内部統制とセキュリティの必要性
- 提案されたプロジェクトの実現可能性調査は，以下のことを含み，どのように作成され，レビューされ，上級管理者によって承認されるべきかにつき述べていること。
    - プロジェクトの環境（ハードウェア，ソフトウェア，テレコミュニケーション）
    - プロジェクトの範囲（最初の，また次の導入で何を含み，何を除外するのか）
    - プロジェクトの制約（たとえ短期間での改善見込みが明らかであっても，このプロジェクトの間に保持されなければならないこと）
    - プロジェクトのスポンサーあるいはオーナ／スポンサーによって実現される利益とコスト

(評価視点続き)

・開発プロセス(即ち，実現可能性の調査の準備，要件定義，システム設計など)の各フェーズが，プロジェクトの次フェーズ(即ち，プログラミング，システム・テスト，トランザクション・テスト，並行テストなど)に移る前に，どのような方法で承認されるべきかを記述していること。
・各プロジェクトに対しSPMPの作成を要求し，プロジェクトの全期間を通じて,プロジェクト時間枠(マイルストーン)と予算により，コントロールがどのように維持されるかについて記述されていること。
・SPMPの組織標準か，もし何も存在しないならば，適切な標準の何れかに準拠すること。
・各プロジェクトに対しSQAPの作成を要求しており，これがSPMPと統合され，すべての関係者によって正式にレビューされ，合意に達していることを保証すること。
・正式なプロジェクト・リスク管理プログラムによって，プロジェクトに関係するリスクがどのように取り除かれるか，または最小限に押さえられるかを記述すること。
・すべての開発，導入，改訂プロジェクトに対し，テスト計画の作成を規定していること。
・すべての開発，導入，改訂プロジェクトに対し，オーナ/スポンサーのスタッフや情報システム機能スタッフを訓練するために，適切な訓練計画の作成を規定していること。

プロジェクト・マイルストーンとコストについての予算対実績が，すべての主なプロジェクト・フェイズ(即ち，ソフトウェア購入，ハードウェア購入，契約プログラミング，ネットワーク・アップグレードなど)を通じて監視され，上級管理者に報告されていること。

予算計上された時間枠と金額を超過したプロジェクトのマイルストーンとコストは，適切な組織管理者により承認される必要があること。

SQAPは，組織のSQAP標準，或いはもし何も存在しないならば，上述の選択基準の何れかに準拠していること。

SQAP保証タスクは，新規，或いは改訂されたシステムの合格基準認定をサポートし，内部統制とセキュリティ機能が要件を満たすことを保証すること。

すべてのプロジェクトのオーナ/スポンサーがSPMPとSQAPの両方に参画し，最終成果物に同意していること。

新規，あるいは改訂された情報システムが計画通りの利益を出していることを保証するためには，導入後プロセスがプロジェクト管理フレームワークの中で必要不可欠な部分であること。

► 準拠性テスト:

プロジェクト管理方法論とすべての要件に基き終始一貫してプロジェクトが遂行されてきたこと。

プロジェクト管理方法論が，そのプロジェクトに携わるすべての適切な要員に伝達されていること。

プロジェクトの性質と範囲に関する定義の記述は，標準のテンプレートに準拠していること。

プロジェクトの定義と認可の際にオーナ/スポンサーの関与した内容と範囲は，プロジェクト管理フレームワークに規定された期待されるオーナ/スポンサーの関与に準拠していること。

スタッフ・メンバのプロジェクトへの任命，プロジェクト・チーム・メンバの責任と権限についての定義は，規定に準拠していること。

プロジェクトの性質と範囲を明白に定義した記述証拠が存在すること，但し，それはプロジェクトの作業が開始される前に定義されていること。

適切な実現可能性の調査が準備され，承認されていること。

(準拠性テスト続き)

開発プロジェクトの各フェイズに対して，適切なオーナ/スポンサーと情報サービス機能管理者の承認が得られていること。

プロジェクトの各フェーズの完了に際して，SPMPの要求通りに，適切な承認が行われていること。

SPMP と SQAPは，プロジェクト管理フレームワークに準拠して開発され承認されること。

SPMPとSQAPは十分詳述され明確であること。

特定された必須の活動/報告書が，実際に実行/作成されてきていること

(即ち経営運営委員会会議，プロジェクト会議などが，定期的に開催されることになっており，会議議事録が作成され，報告書が作成され，それらが適切な関係者に配付されていること)。

テスト計画は，プロジェクト管理フレームワークに準拠して作成され，承認されてきており，詳述され，充分明確であること。

テスト計画で明らかにされた必須の活動/報告書が実際に実行/作成されていること。

プロジェクトで使用される合格認定基準が存在し，それは，：

- ･目標と業績指標から得られていること。
- ･合意された定量的要件から得られていること。
- ･内部統制とセキュリティ要件が満たされていることを保証すること。
- ･絶対必要な『 What 』に対する任意の『 How 』の関連があること。
- ･正式な合格/不合格のプロセスを定めること。
- ･限られた時間の範囲内で客観的なデモンストレーションができること。
- ･設計文書の要件を単に言い換えないこと。

プロジェクト･リスク管理プログラムが，プロジェクトに関係するリスクを明らかにし，除去し，あるいは少なくとも最小化するために使われていること。

テスト計画が守られ，オーナ/スポンサー，プログラミングと品質保証機能によってテスト･レビュー文書が作成され，承認プロセスが意図された内容に準拠していること。

影響を受けるオーナ/スポンサーと情報システム機能のスタッフを訓練するための計画が文書で作成され，必要な訓練活動を完了するために十分な時間が与えられ，その計画がプロジェクトで使用されていること。

導入後レビュー計画が遵守され，プロジェクトのために実行されていること。

► 実証性テスト:

類似した組織や適切な国際標準／承認された業界の最も良い慣行に対して，プロジェクト管理フレームワークのベンチマークを実施すること。

以下について詳細なレビューを実施すること：

- ･プロジェクト･マスタ計画，即ち，オーナ/スポンサーの関与すべき範囲を決定し，下記にあげるものを含み，プロジェクトの定義，承認，実行といった一般的なプロセスの適切性を決定する
  - ･システム機能の定義
  - ･プロジェクトの実現可能性，所与の制約
  - ･システムのコストと効果の決定
  - ･システム･コントロールの適切性

(実証性テスト続き)

- 他のオーナ/スポンサーのシステムへの影響並びに統合
- 資源 (要員と資金) に対するオーナ/スポンサーの公約
- プロジェクト参加者の責任と権限の定義
- 検収基準が望ましく, 達成可能なものであること
- プロジェクト・フェーズの承認に, マイルストーンとチェックポイントの使用
- プロジェクト管理にガントチャート, 事故報告書, 会議要約などの使用

- 組織のシステム品質保証計画策定プロセスに組織的な問題が存在するかどうかを見極めるための品質報告書
- 諸リスクが明らかにされ, 排除され, あるいは少なくとも最小化されてきたかどうかを見極めるための正式なプロジェクト・リスク管理プログラム
- システム全体の開発, 導入, あるいは改訂といったプロジェクトにおいて, テストが徹底的になされたかどうかを見極めるためのテスト計画の実施状況
- システムの使用に際し, オーナ／スポンサーや情報システム機能のスタッフを十分に教育したかどうかを見極めるための訓練計画の実施状況
- プロジェクトの計画対実績利益が確かめられたかどうかを決定するための導入後レビュー

► 実証性テストの結果:

プロジェクトの状態:

- 管理が不十分である
- マイルストーン期日を過ぎている
- 予定コストを上回っている
- 逃げのプロジェクトである
- 承認されていない
- 技術的に実現可能性がない
- コストが正当化されていない
- 計画された利益を達成していない
- チェックポイントを含んでいない
- 重要なチェックポイントで承認されていない
- 実施についての承認がなされていない
- 内部統制並びにセキュリティ要件が満たされていない
- リスクが排除されていないか, または減少していない
- 徹底的にテストされていない
- 導入システムに対して必要な訓練がなされなかったか, または訓練は不適切であった
- 導入後レビューが行なわれなかった

PO11 品質管理

コントロール目標
11.01 全般的品質計画
11.02 品質保証の方法論
11.03 品質保証の計画策定
11.04 情報サービス機能の標準および手続への準拠に関する品質保証レビュー
11.05 システム開発ライフサイクル方法論
11.06 既存技術への大幅な変更に対するシステム開発ライフサイクル方法論
11.07 システム開発ライフサイクル方法論の更新
11.08 調整と伝達
11.09 技術基盤に関する取得と維持のフレームワーク
11.10 第三者機関による実施者の関係
11.11 プログラムの文書化標準
11.12 プログラムテスト標準
11.13 システムテスト標準
11.14 並行／パイロットテスト
11.15 システムテストの文書化
11.16 開発標準に対する準拠性の品質保証評価
11.17 情報サービス機能の目標達成の品質保証レビュー
11.18 品質測定基準
11.19 品質保証レビューの報告書

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

最高経営責任者
情報サービス機能の計画策定/運営委員会メンバ
情報統括役員
セキュリティ担当役員
組織の品質管理者
情報サービス機能の品質管理者
情報サービス機能の管理者
システム・オーナ/スポンサー

収集すべき証拠資料:

品質保証, システム開発ライフサイクル, システム文書化に関連した方針および手続き
上級管理者の運営の役割と責任
組織の戦略計画, 品質方針, 品質マニュアル, 品質計画
情報サービス機能の戦略計画, 品質方針, 品質マニュアル, 品質計画, 構成管理計画
すべての品質保証機能の規定
個々の品質計画会議の議事録

(収集すべき証拠資料続き)

システム開発ライフサイクル方法論をレビューするために招集された会議の議事録
システム開発ライフサイクル方法論のレビューのコピー
状況報告書および計画策定/運営委員会の会議議事録

評価視点:

品質計画が:

- ・組織の長期/短期計画に基づいていること
- ・改善の哲学を推進し続け，何を/誰が/どのようにといった基本的な質問に答えていること。
- ・完全であり最新であること。

情報サービス機能の品質計画が:

- ・組織の全般的な品質計画と情報技術の長期/短期計画に基づいていること。
- ・改善の哲学を推進し続け，何を，誰が，どのようにといった基本的な質問に答えていること。
- ・完全であり最新であること。

品質保証に対する標準的な方法が存在し，その方法が:

- ・品質保証活動に関して，一般的なものまたはプロジェクト特有なもの両者に適用可能であること。
- ・拡大縮小可能であり，従ってすべてのプロジェクトに適用可能であること。
- ・プロジェクト並びに品質保証活動に関わるすべての個々人により理解されていること。
- ・プロジェクトのすべてのフェーズを通して適用されていること。

全般的な品質計画の目的達成のために行われるべき品質保証活動のタイプ(並びに明確なレビュー，監査，検査，等)を，品質保証に関する標準的な方法によって規定すること。

品質保証計画によって，品質保証活動の範囲とタイミングが規定されること。

品質保証のレビューによって，情報サービス機能の標準，方針，手続きに対する全般的な準拠性を評価すること。

上級管理者が情報サービスの標準，方針，手続きを決定し導入していること。それらには，外部調達，独自開発，もしくは両者の組合せを対象とした正式なシステム開発ライフサイクル方法論が含まれること。

システム開発ライフサイクル方法論が:

- ・コンピュータ化された情報システムおよび関連する技術の開発，取得，導入および保守のプロセスを管理していること。
- ・組織および情報サービス機能の長期/短期計画に準拠する開発，改訂の企てをサポートし促進していること。
- ・構造化された開発，または改訂プロセスを要求し，それらには，重要な決定がなされる個所にチェックポイントが有り，各チェックポイントでプロジェクト進行の承認が必要とされていること。
- ・完全かつ最新であること。
- ・組織内で必要な開発のすべてのタイプに適用できるように，調整/拡大縮小可能であること。
- ・内製および購入ソフトウェア双方の構築と保守に対して適用可能であること。

(評価視点続き)

・技術変更規程を文書化していること。
・技術基盤の取得と維持に関しては，全般的なフレームワークを組み込んでいること。
・遵守すべき諸々のステップ(取得；プログラミング，文書化，テスト；パラメータ設定；保守および修正の適用)は，技術基盤の取得と保守のフレームワークに依って統制され整合性が保持されていること。
・第三者機関の導入者に関しては，次の各々を概説した規定を要求すること：
検収基準，変更処理，問題処理，参加者の役割，設備，ツールおよびソフトウェアの標準と手続き。
・詳細なプログラムとシステム文書（即ち，フローチャート，データ・フロー・ダイアグラム，記述されたプログラムの説明部，等）の維持を要求しており，それらの要求はすべての関連するスタッフに伝達されていること。
・文書が，変更の生ずる都度，最新版に保たれることを要求すること。
・厳格で強靭なプログラム・テスト，システム・テストの適用を要求すること。
・新規もしくは改訂されたシステムの並行又はパイロット・テストの実施環境を決定すること。
・テストが独立性を保って検証され，文書化され，維持されることを，すべてのシステム開発，導入または改訂プロジェクトの一部として位置づけて要求すること。

組織の品質保証方法により：
・すべての新規もしくは改訂されたシステムは，組織のシステム開発ライフサイクル方法論に準拠して開発され，稼動しており，又その方法論はプロジェクトチームにより遵守されてきていることを保証するために，導入後レビューの実施を要求すること。
・管理者により設定された目標に対して，新規もしくは改訂されたシステムの達成度をレビューすることを要求すること。
・管理者(ユーザと情報サービス機能の双方)に対して，システム開発と有効性の勧告を，報告書で適切に行なうこと。
・勧告を定期的にフォローアップし，適切な上級管理職役員に報告すること。

情報サービス機能の上級管理者は，新規開発/改訂や新しい技術に対する適切性を確かめるために，定期的にシステム開発ライフサイクル方法論をレビューしかつ適切に更新すること。

種々のタイプの開発および保守プロジェクトに対して，多様な管理レベルが設定されていること。
（例えば，大規模プロジェクトは小規模プロジェクトに比して，より多くのコントロールが必要）

システム開発ライフサイクル全体を通して，情報サービス機能の顧客とシステム導入者間で，密接な調整と意志の疎通がなされていること。

組織内の異なる機能/個々人の間に適切な関わり合いができていること（例：情報サービス機能管理者，セキュリティ役員，法務スタッフ，品質保証スタッフ，監査スタッフ，ユーザ，等）

行動の結果を測定するための測定基準が存在し，品質目標が達成されたかを評価可能ならしめること。

準拠性テスト:

情報サービス機能の品質計画を策定する手続きには，入力として以下が含まれているか。

- ･組織の長期/短期計画
- ･情報サービス機能の長期/短期計画
- ･組織の品質方針
- ･情報サービス機能の品質方針
- ･組織の品質計画
- ･情報サービス機能の構成管理計画

情報サービス機能の品質計画は，下記を定義する情報サービス機能の長期/短期計画に基づいているか。

- ･アプリケーション･システム開発の成果および/または取得
- ･他システム（内部および外部）とのインタフェース
- ･システムおよびインタフェースのサポートに必要な情報サービス機能のプラットフォーム/基盤
- ･目標とする情報サービス機能環境を開発/支援するための資源（資金と人材）
- ･目標とする情報サービス機能環境を開発/支援するのに必要な訓練

情報サービス機能の品質計画は，下記を考慮しているか。

- ･顧客（内部もしくは外部）に提供されるべき目標とするサービスの水準は，明確に測定可能なこと
- ･各々のシステムやプラットフォームに関して目標とする許容停止時間の最大は，明確に測定可能なこと
- ･目標とするパフォーマンス，許容停止最長時間を監視するのに必要なパフォーマンス統計，それらはどのようにして報告され，誰に配付されるべきかも含む
- ･情報サービス機能の長期/短期計画で示される情報サービス機能の環境/基盤下での開発/改訂/移行が，良好な状態で計画/監視/資源調達/テスト/訓練/文書化/導入されることを保証するのに必要な監視とレビューのプロセス
- ･品質計画が更新される間隔

品質保証要員が，品質保証の方法，計画，その他の確立された運用手続きを終始一貫して遵守しているか。

適切なシステム開発ライフサイクル方法論によって以下が保証されているか。

- ･新規システムと新しい技術に対する開発プロセスを通じての充分なコントロール
- ･システムの開発および保守に携わるすべての適切な要員に対する意志疎通
- ･技術上の変更に対する手続きの利用
- ･ユーザの受諾と承認を保証する手続きの利用
- ･第三者機関導入者との契約の適切性

ユーザが，システム開発ライフサイクル方法論のコントロールと要件を理解しているか。

システム開発ライフサイクル方法論内の変更管理メカニズムは，変更が方法論に対しても及ぶことを可能にしているか，また，その方法論は現在用いられているものであるか。

組織のシステム開発ライフサイクル方法論の改訂および変更記録が，現在検討中で将来必要な新規システムおよび新技術を反映しているか。

完成プログラム並びにシステムのテスト結果（並行/パイロット･テスト結果を含む）がレビューされ，将来のテストのために保管されているか。

(準拠性テスト続き)

テスト中に直面した問題を解決するための手続きは適切であるか。
導入後のレビューが，品質保証スタッフによって実施されているか。
システム開発プロジェクトに関わっているユーザ部門の代表は，方法論の現在の使用に満足しているか。
品質保証スタッフは，組織内での自分達の役割を明確に理解しているか。
すべてのシステム・テスト，テスト結果のレビュー，並びに適切な情報サービス機能の管理者/品質保証/ユーザ要員による承認，これら各々の完了直後に品質保証レビューを実施することを要求しているか。
品質保証レビューの結果が，管理職による改善活動に結びついているか。
導入後のレビューが実施され，結果が上級管理者に伝達され，改善を求められているすべての実施領域に対して活動計画が要求されているか。
品質目標に対して，結果が測定され，行動を伴っているか。

実証性テスト:

システム開発ライフサイクル方法論について，類似した組織や適切な国際標準/業界最良と認められた慣行とのベンチマークを実施すること。
品質計画に含まれるパフォーマンス対策を詳細にレビューし，以下の通りであることを確認する。
- ・達成可能であること
- ・その企業の要求/期待に対処していること
- ・ユーザの要求/期待に対処していること
- ・測定可能であること

サンプリングされたプロジェクトを詳細にレビューし，以下が保証されていることを確認する。
- ・システム開発ライフサイクル方法論に準拠していること。
- ・システム開発ライフサイクル方法論の調整/拡大縮小は適切であり，承認されたものであること
- ・すべてのチェックポイントですべての重要なコントロール要員（例えば，情報サービス機能のセキュリティ役員，品質保証要員，ユーザ代表者）による承認が得られていること
- ・情報サービス機能のユーザとシステム導入者（社内または第三者機関）の間で密接な調整と意志疎通が図られていること
- ・技術的基盤並びに関連したすべてのステップに関する取得と保守のフレームワークが遵守されていること
- ・開発／改訂が，満足できる状態でタイムリーに完了していること
- ・適切な品質保証レビューの報告が行われ，すべての必要な是正活動がタイムリーに行なわれていること

プログラムとシステム関連文書が，どのような方法で作成され，レビューされ，承認され，維持されているかについて，詳細なレビューが実施されていること。
プログラム・テスト，システム・テスト（並行/パイロット テストを含む），文書化がどのような方法で準備され，レビューされ，承認され，維持されているかについて詳細なレビューが実施されていること。

(実証性テスト続き)

品質保証の導入後レビュー・プロセスについて詳細なレビューを実施し，以下が報告書によって取り扱われるようになっていることを保証すること：

システム開発ライフサイクルプロセス規程への準拠性

新規導入/改訂されたシステムの有効性と品質についての評価

► 実証性テストの結果:

長期/短期計画に無関係な品質計画の存在。

システム開発ライフサイクル方法論を使用しない例，システム開発ライフサイクル方法論を濫用している例。(例えば，小規模プロジェクトで構造化を濫用，大規模プロジェクトでの不十分な構造化) システム開発ライフサイクル方法論の不適切な使用。
(例えば，修正を必要としない既製のソフトウェア・パッケージの導入に際して，自社開発の場合に使用すべきシステム開発ライフサイクル方法論を適用)

システム開発ライフサイクル・プロセスに関係する個々人 (第三者機関導入者を含む) の間で調整と意志疎通が貧弱であるか，または存在しない例。

技術基盤の取得と維持において異なるステップを取る必要が有る場合に (例えば，取得；プログラミング，文書化とテスト；パラメータ設定；保守と修正適用) ，それらが適切に遵守されていない。

プログラム文書，システム文書が存在しないか，不適切か，最新でない。

プログラム・テスト，システム・テスト (並行/パイロット・テストを含む) が実施されなかったか，実施が不適切であったか，文書化されなかったか，文書化が不適切であった。

品質保証レビュー/導入後のレビューが，実施されなかったか，実施が不適切であった。

品質保証レビュー/導入後のレビューが，管理職に無視され，望ましくないシステムが導入された。

取得と実施

AI1 解決法の識別

コントロール目標
1 情報要件の定義
2 代替行動の定式化
3 取得戦略の立案
4 第三者機関のサービスの要件
5 技術的実行可能性の検討
6 経済的実行可能性の検討
7 情報アーキテクチャ
8 リスク分析報告書
9 コスト効果のあるセキュリティ・コントロール
10 監査証跡の設計
11 人間工学
12 システム・ソフトウェアの選択
13 調達のコントロール
14 ソフトウェア製品の取得
15 第三者機関のソフトウェアの保守
16 アプリケーション・プログラミングの契約
17 ファシリティの受理
18 技術の受理

高いレベルと詳細コントロール目標の監査手続

理解

面接対象者:

情報統括役員
セキュリティ管理者
情報サービス部門の上級管理者
プロジェクト オーナ／スポンサー
契約管理者

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調達に関する方針と手続
ITの目標と長期/短期計画
以下のサンプリングされたプロジェクト文書
要件定義，代替案分析，技術的実現可能性の検討，経済的実現可能性の検討書，情報アーキテクチャー／企業データ・モデルの分析書，リスク分析書，内部統制／セキュリティのコスト対効果の検討書，監査証跡分析書，人間工学の検討書，施設と特定技術の検収計画とテスト結果
ソフトウェアの購入，開発，保守に関するサンプリングされた契約書

コントロール評価

► 評価視点:

方針と手続は以下の要件を要求:

- ･既存システムにより満たされている，または提案された新規あるいは改訂システムによって満されるであろうユーザ要件は，開発/導入/改訂プロジェクトが承認される前に，明確に定義されていること
- ･開発，導入，改訂プロジェクトが承認される前に，ユーザ要件ドキュメンテーションが適切なオーナ／スポンサーによってレビューされ，書面で承認されること
- ･解決策の機能要件と運用要件は，性能，安全性，信頼性，互換性，セキュリティ，法律の諸条件を含めて満足できるものであること
- ･ユーザ要件に対しあるソフトウェア解決案を選択する前に，代替解決案が検討され，分析されていること
- ･最終的な選択の決定がなされる前に，個々のシステム開発，改訂プロジェクトに関してユーザ要件を満足する商用ソフトウェア･パッケージが識別されていること
- ･ソフトウェア･プロダクトの取得に関する代替案は，既製プロダクト購入か，内製か，契約を介してか，既存ソフトウェアの拡張か，或いはこれらすべての組み合せによるかの見地から明確に定義されていること
- ･提案された新規，または改訂システム･プロジェクトの開発に関して確立されたユーザ要件を満足する各代替案について，技術的実現可能性の検討が準備され，分析され，該当のオーナ／スポンサーによって承認されること
- ･各々の提案されたシステム開発，導入，改訂プロジェクトにおいて，ユーザ要件を満足する各代替案に関してコスト対効果の分析が行なわれること
- ･提案された新規，あるいは改訂システム･プロジェクトに関して，開発か改訂かどちらにするかという決定を行う前に，経済的実現可能性の検討が準備され，分析され，該当のオーナ／スポンサーによって承認されること
- ･解決案が識別され，実現可能性が分析される際に，企業データ･モデルに注意を払うこと
- ･各々の提案されたシステム開発，導入，改訂プロジェクトにおいて，セキュリティの脅威，潜在的な脆弱性と影響，識別されたリスクを減少または除去する為に実現可能なセキュリティと内部統制による安全保護，これらについての分析が準備され，文書化されていること
- ･管理コストが利益を上回らないことを保証するために，セキュリティのコスト対効果が慎重に検討されていること
- ･コスト対効果の検討に関し，管理者が正式に署名していること
- ･プロジェクトの設計フェーズにおいて，すべての提案された新規あるいは改訂システムに適切な監査証跡とコントロールが組み込まれることを要求していること
- ･監査証跡と統制は，システム･セキュリティを危うくすること無しに，他ユーザにより（例，匿名，偽りの匿名，無関係，観察できない等の行為に依る）自分達の身元を発見されたり，誤使用されたりするのを防ぐ可能性を提供すること
- ･各々の提案されたシステム開発，導入，改訂プロジェクトは，自動化されたシステムの導入に関連する人間工学の問題に注意を払うこと
- ･情報サービス部門の管理者は，その運用要件を満足させる可能性のあるすべてのシステム･ソフトウェア･プログラムを識別すること

(評価視点続き)

・製品は，使用され財務決済される前に，レビューされ，テストされること
・ソフトウェア製品の取得は，提案書作成要求，ソフトウエア製品提供者の選定，契約交渉，これらに関するフレームワークを設定している組織の調達方針に従うこと。
・第三者機関の供給者から取得したライセンス・ソフトウェアに対して，供給者はソフトウェア製品のインテグリティの正しさを検査し，保護し，維持するための適切な手続をもつこと
・契約プログラミング・サービスの調達は，情報サービス部門の任命されたメンバからのサービスに対する文書による要請をもって正当化されること
・施設の検収計画は契約書によって供給者と同意されており，この計画には検収手続と検収基準が定義されていること
・完了した契約プログラミング・サービスの最終製品は，その作業に対する支払と最終製品の承認前に，情報サービス部門の品質保証グループと他の関係者によって関連する基準に従ってテストされレビューされること
・特定の技術に対する検収計画が契約書によって供給者と同意され，この計画には検収手続と検収基準が定義されていること

リスク分析は，全体的なリスク評価フレームワークに従って行われること
搬出/搬入データ(exported and imported data)に対し，セキュリティ属性を割り当て，維持し，それらのデータを正しく解釈する為の仕組みが存在すること
管理者は，ITのハードウェア/ソフトウェア/サービスの調達に際し，遵守しなければならない共通の手続と基準について記述した中心的調達アプローチを開発し導入していること
契約書には，ソフトウェア，ドキュメンテーション，他の成果物を，受領する前にテストし，レビューすることを規定していること
契約の明細に含まれるテストには以下を含めること ：

システム・テスト，統合テスト，ハードウェアと構成要素テスト，手続テスト，負荷とストレステスト，チューニングと性能テスト，回帰テスト，ユーザ検収テスト，予期せぬシステム障害を避ける為のシステム全体のパイロット・テスト

設備と環境が契約の明細に述べられた要件に応じていることを保証する為に，施設の検収テストが行われること
特定の技術の検収テストには検査テスト，機能テスト，作業負荷テストが含まれること

準拠性評価

準拠性テスト:

プロジェクトが開発，導入，あるいは改訂される前に，既存システムによって満たされ，提案された新規，または改訂システムによって満たされるであろうユーザ要件が，適切なユーザによって明確に定義され，レビューされ，書面によって承認されていること
解決策の機能要件，運用要件は，性能，安全性，信頼性，互換性，セキュリティ，法律の諸条件も含め満足ゆくものであること
既存システムのすべての弱点と処理上の欠陥が識別されていて，提案された新規，あるいは改訂システムによって完全に対応され，解決されるようになっていること

(準拠性テスト続き)

提案された新規，あるいは改訂システムに関して確立されたユーザ要件を満たすであろう代替的活動方針が適切に分析されていること

特定のシステム開発や改訂プロジェクトのニーズを満足する商用ソフトウェア・パッケージが，適切に識別され，考慮されていること

各々の代替案に関係するすべての識別できるコストと効果が，適切に支持され，そして要求される経済的実現可能性検討の一部分として含まれていること

解決策が特定され，実現可能性の分析が行われた際にも，情報アーキテクチャ／企業データ・モデルに注意が払われていること

セキュリティの脅威，潜在的な脆弱性と影響，そして識別されたリスクを減少または除去させる為の実現可能なセキュリティと内部統制による防護対策，これらに関するリスク分析報告書は正確であり，包括的であること

セキュリティと内部統制の問題が，システム設計文書の中で適切に扱われていること

設置したコントロールおよび計画されたコントロールは十分であり，コストを補うに十分な利益があるものであることを管理者は是認していること

特定され，選択された解決策に対して監査証跡の為の適切な仕組が利用可能であるか，または開発され得るものであること

エンド・ユーザ・スキルを高める為のユーザ・フレンドリな設計が，システム設計，画面レイアウト/帳票フォーマット/オンライン・ヘルプ機能などの開発の際に考慮されていること

人間工学の問題が，システムの設計や開発を行う際に考慮されていること

利用時の性能の問題（即ち，システム応答時間，ダウンロード／アップロード能力，非定型レポーティング）が，設計や開発を行う前にシステム要件仕様書で取り扱われていること

運用要件を満足させる可能性のあるすべてのシステム・ソフトウェア・プログラムが情報サービス部門により識別されていること

IT関連のハードウェア，ソフトウェア，サービスの調達においては，情報サービス部門は共通の手続と標準を遵守すること

購入製品は，使用され財務決済される前に，レビューされ，テストされること

もし適用可能ならば，ソフトウェア購入契約において，ユーザがプログラム・ソース・コードのコピーを持てるようにすること

ソフトウェア製品のアップグレード，技術の更改と修正が，調達ドキュメントに明細に述べられていること

第三者機関によるソフトウェアの保守には，そのソフトウェア製品のインティグリティの検証，保護，維持の諸要件を含むこと

契約プログラミング要員の作業は，その組織のプログラマーに要求されるのと同じレベルのテスト，レビュー，承認の要求に従がわなければならないこと

組織の品質保証部門は，契約プログラマーによって行なわれた作業のレビューと承認に対して責任をもつこと

施設検収計画は，検収の為の手続と基準を含み適切性と完全性が保持されていること

特定の技術の検収計画は，検査，機能性テスト，作業負荷テストを含み，適切性と完全性が保持されていること

実証性テスト:

類似した組織や適切な国際標準／認められた業界の最良の慣行に対して，ユーザ要件を満たす自動化された解決法についてのベンチマークを行うこと

以下について詳細なレビューを行うこと ：

- ユーザ要件を満たす自動化された解決法の確認（次を含む： ユーザ要件の定義，代替行動方針の立案； 商用ソフトウェア・パッケージの識別；技術的実現可能性/経済的実現可能性/情報アーキテクチャ/リスク分析の検討についての作業）
- 識別され，選択された解決案に対して利用可能な，または開発され得るセキュリティ，内部統制（ユーザフレンドリーな設計，人間工学などに対する考慮も含む），監査証跡
- システム・ソフトウェアの選択と導入
- 組織のソフトウェアの既存の調達方針と手続，並びに内部統制の適切性と準拠性
- 第三者機関による保守に対する管理方法
- 契約アプリケーション・プログラミングに対する監視と管理の方法
- 設備および環境テストが契約で特定された要件を満たすことを保証する為の施設検収プロセス
- 検査，機能性テスト，作業負荷テストが，契約書で明細に述べられた要件を満たすことを保証する特定の技術の検収プロセス

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方法論に欠陥があること

解決策がユーザ要件を満たさないこと

以下のシステム開発への取組み：

- 代替策を検討しなかった結果，より高価な解決策となってしまったこと
- より短期間に，より少ないコストで導入できたはずの商用ソフトウェア・パッケージを検討しなかったこと
- 代替的な技術的実現可能性を検討しなかった，あるいは選択された解決策の技術的実現可能性を不適切に検討してしまった結果，当初設計された通りの解決策を導入できなかったこと
- 経済的実現可能性の検討の際に誤った仮定をしてしまい，その為に間違った実行方針を選択してしまったこと
- 情報アーキテクチャ／企業データ・モデルを検討しなかった結果として間違った実行方針を選択してしまったこと
- 確としたリスク分析を行わなかった為に，適切にリスク（脅威，潜在的な脆弱性と影響を含む）を特定しなかったか，または識別されたリスクの減少や除去の為の適切なセキュリティや内部統制を特定しなかったこと

以下の結果をもたらした解決策：

- コントロールとセキュリティのコスト対効果の検討が不適当だったことによる過剰なコントロール，あるいは過小なコントロールが行なわれたこと
- 適切な監査証跡を持たなかったこと

(実証性テストの結果続き)

・ユーザ・フレンドリーな設計と人間工学の問題を検討しなかった為に，避けることができたであろうデータ入力エラーを引き起こしていること
・組織内で確立された調達アプローチに従わなかった為に，組織にコストの追加を生じさせていること

必要なシステム・ソフトウェアが欠如していること

パラメータの設定が不適切だった為に，システム・ソフトウェアが有効でなくなったこと

契約条件を遵守しなかった第三者機関によるソフトウェア保守の結果，組織の使命，目標達成の上で不利な影響をこうむっていること

契約条件を遵守しなかった契約アプリケーション・プログラミングの結果として，組織に追加コストを支払わせたり，システム導入を遅れさせたりしたこと

設備環境を十分にテストすること無しに検収してしまった結果として，ユーザ要件が満たされていなかったり，契約条件が遵守されていなかったりしたこと

特定技術の受け入れの際に，検査，機能性テスト，作業負荷テストが適切に行なわれなかった為に，結果として，その技術はユーザ要件を満足していなかったり，契約条件を遵守していないかったりしたこと

何らかのシステム障害が発生していること

AI2 アプリケーション・ソフトウェアの取得と保守

コントロール目標
1 設計方法
2 既存システムに対する大幅な変更
3 設計の承認
4 ファイルの要件定義と文書化
5 プログラム仕様
6 原始データの収集設計
7 入力の要件定義と文書化
8 インタフェースの定義
9 ユーザ・マシン・インタフェース
10 処理の要件定義と文書化
11 出力の要件定義と文書化
12 管理可能性
13 重要な設計要素としての可用性
14 アプリケーション・プログラム・ソフトウェアにおけるITのインティグリティ条項
15 アプリケーション・ソフトウェアのテスト
16 ユーザの参照資料と支援資料
17 システム設計の再評価

高いレベルと詳細コントロール目標の監査手続

理解

面接対象者:

情報統括役員
セキュリティ管理者
情報サービス部門の上級管理者
プロジェクト オーナ／スポンサー

収集すべき証拠資料:

システム開発ライフサイクル方法論に関する方針と手続
ITの目標と長期/短期計画
サンプリングされたプロジェクトに関する以下の文書
設計承認, ファイル要件定義, プログラム仕様書, ソース・データの収集設計, 入力要件定義, ユーザ・マシン・インタフェース, 処理要件定義, 出力要件定義, 内部統制／セキュリティ要件, 可用性要件, ITインティグリティ規程, アプリケーション・ソフトウェアのテスト計画と結果, ユーザ参照資料と支援資料, システム設計の再評価

コントロール評価

► 評価視点:

方針と手続は，以下を保証すること ：

- ･組織のシステム開発ライフサイクル方法論は，新規システムの開発，既存システムへの大幅な変更，ユーザの参画に適用されること
- ･設計仕様書を作成し，ユーザ要件と対照して設計仕様書を検証する際にユーザと緊密な連絡を保つこと
- ･既存のシステムに対し大幅な変更がなされる場合には，新規システム開発の場合と同じと考えて，同様のシステム開発ライフサイクル･プロセスを遵守すること
- ･すべての新規システム開発や改訂プロジェクトの設計仕様書が，管理者，影響を受けるユーザ部門，組織の上級管理者によって承認されること
- ･各々の新規システム開発あるいは改訂プロジェクトにおいて，ファイル･フォーマットを定義し，文書化を行うに際しては，データ･ディクショナリ規則の遵守といった要件を含め，適切なプロセスを適用すること
- ･詳細に文書化されたプログラム仕様書が，各々のシステム開発や改訂プロジェクトに対して用意され，これらのプログラム仕様書はシステム設計仕様書に一致していること
- ･各々の新規システム開発あるいは改訂プロジェクトに対して，データの収集と入力の為の適切な仕組みが明細に記述されていること
- ･各々の新規システム開発あるいは改訂プロジェクトに対して，入力要件を定義し，文書化する為の適切な仕組みが存在すること
- ･(オンラインヘルプ機能によって) 簡単に使え，自動的に自己文書化されるユーザ･マシン･インタフェースの開発が存在すること
- ･各々の新規システム開発，改訂プロジェクトに対して，内部並びに外部インタフェースを定義し文書化する為の適切な仕組みが存在すること
- ･各々の新規システム開発あるいは改訂プロジェクトに対して，処理要件を定義し，文書化する為の適切な仕組みが存在すること
- ･各々の新規システム開発あるいは改訂プロジェクトに対して，出力要件を定義し，文書化する為の適切な仕組みが存在すること
- ･各々の新規システム開発あるいは改訂プロジェクトに対して，内部統制とセキュリティ要件を保証する為の適切な仕組みが明細に記述されていること
- ･内部統制とセキュリティ要件は，入力と出力の正確性／完全性／適時性／正当性 (承認) を保証するアプリケーション統制を含むこと
- ･新規，あるいは改訂システムの設計プロセスにおける可能な限り早い段階で，可用性を検討すること，そしてこの検討では，保守性と信頼性を分析し必要に応じ改善を図ること
- ･アプリケーション･プログラムには，ソフトウェアによって実行されるタスクを日常的に検証し，ロールバックやその他の手段を介してインティグリティの復旧の備えをする規定が存在すること
- ･アプリケーション･ソフトウェアは，ユーザによって承認される前に，プロジェクト･テスト計画や確立されたテスト標準に従ってテストされること
- ･すべてのシステム開発あるいは改訂プロセスの一部として，適切なユーザ参照/支援マニュアルが用意されること (なるべく電子フォーマットで)

(評価視点続き)

・システム開発や保守段階において，重要な技術的，論理的な矛盾が生じた際はその都度，システム設計を再評価すること

ユーザの参照資料，支援資料の正確かつタイムリーな更新が，システム開発ライフサイクル方法論により確保されること

新規システム開発あるいは改訂プロセスの開始の際に機密性評価の実施を，システム開発ライフ・サイクル方法論は義務づけていること

新規開発または改訂されるシステムの基本的なセキュリティと内部統制の側面は，できるだけ早い時期にセキュリティの概念を設計に組込む為に，システムの概念設計とともに評価されることをシステム開発ライフサイクル方法論は義務づけること

論理的セキュリティとアプリケーション・セキュリティの問題が，新規システムの設計，既存システムの改訂時に確認され含められるべきである事を，システム開発ライフサイクル方法論は義務づけること

セキュリティと内部統制面についての評価は，健全なフレイムワークに基づくこと

人工知能システムは，重要な決定が承認されている事を保証する為に，オペレータとのインタラクションまたはコントロール・フレイムワークの基に置かれること

アプリケーション・テストの際に使用される機密データ開示を減らすために，強力なアクセス制限を行うか，または使用される履歴データの非個人化 (個人特定の防止) によること

準拠性評価

▶準拠性テスト:

システム開発ライフサイクル・プロセスにおけるユーザの参加が多いこと

システム設計上のすべての問題 (即ち，入力，処理，出力，内部統制，セキュリティ，災害時回復，応答時間，レポーティング，変更管理など) を適切に取り扱うプロセスが存在することを組織のシステム開発ライフサイクル方法論は保証すること

重要なシステム・ユーザが，システム設計プロセスに参加すること

設計レビューと承認プロセスにおいては，プロジェクトの次フェーズの作業を始める前に，すべての問題が解決されてきていることを保証すること

既存システムで大幅な変更がなされる際は，新規システムの開発のために使われたのと同様のシステム開発ライフサイクル方法論を使ってシステムが開発されることを保証すること

システムのプログラミングは，設計に対する承認が正式に得られるまで開始できないないことを，設計承認手続で保証すること

システムのファイル要件と文書化，並びにデータ・ディクショナリは，すべて標準と整合性を保つこと

最終ファイル仕様書にユーザ署名があること

プログラム仕様書がシステム設計仕様書に一致していること

データ収集設計仕様書とデータ入力設計仕様書が一致すること

ユーザ・マシン・インタフェース設計仕様書が存在すること

ユーザ・マシン仕様書では，使用し易く (オンライン・ヘルプ機能を使った) 自己文書化機能が使用されていること

内部並びに外部インタフェースが文書化されていること

処理要件が設計仕様書に記述されていること

(準拠性テスト続き)

出力要件が設計仕様書に記述されていること
内部統制とセキュリティ要件が設計仕様書に記述されていること
入力と出力に対する正確性，完全性，適時性，および正当性（承認）を，アプリケーション統制要件設計仕様書で保証すること
内部統制とセキュリティ要件を（新規システムあるいは改訂システム何れであろうと），できるだけ早い時期にシステムの概念設計に含めること
セキュリティ管理者が，新規システム，あるいはシステム改訂プロジェクトのシステム設計，開発，導入プロセスに積極的に関わっていること
改善された可用性/信頼性が，もし適用可能ならば，時間および以前の方法よりもより効果的な手続によって計量化されてきたかどうかを，システム設計で決定すること
アプリケーション・プログラム規程により，データ・インティグリティの保証を支援するソフトウェアによって実行される作業を定常的に検証すること
確立されたテスト標準が存在すること
プロジェクト・テスト計画とユーザ承認プロセスが存在すること
ユーザの参照資料，支援資料，オンライン・ヘルプ機能が利用できること
ヘルプ・デスク部門がより複雑な処理問題に対処できるように，効果的にユーザを支援していること
利用者窓口における問題の上申手続には，追跡，監視，適切な情報サービス部門管理者へのそれら問題の報告が含まれること
ユーザ・ドキュメンテーションを更新する適切な仕組みが要求されていること
ユーザ・ドキュメンテーションの変更に際して連絡が行なわれていること
重要な技術的，論理的な矛盾が発生する都度，再評価プロセスに沿って処理されること

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:

アプリケーション・ソフトウェアの取得と開発に要するコストを，類似した組織あるいは適切な国際的な標準／認められた業界のベスト・プラクティスに対して，ベンチマークを実施すること
プロジェクトをサンプリングし，以下につき詳細なレビューを実施すること：

- ・設計仕様書の適切性と，それら仕様書への設計の準拠性を評価する為のシステム設計文書
- ・新規システム開発，改訂プロジェクトにおいて設計仕様書文書が， 情報サービス部門の管理者と影響を受けるユーザ部門の管理者のみならず，適切ならば組織の上級管理者によってもレビューされ，承認されてきたかどうかの判定
- ・ファイル要件（少なくとも下記のファイルに対して）が，プロジェクト導入チームによって明確に理解され，システム要件／ユーザ要件／組織のデータ・ディクショナリ規程毎に組み立てられていることを保証する為のソフトウェア文書
- ・マスタ
- ・トランザクション
- ・コマンド
- ・プログラム
- ・コントロール
- ・テーブル

(実証性テスト続き)

- ・レポート
- ・プリント
- ・ログ
- ・伝送
- ・フロー・チャート/フロー・ダイアグラムで識別されるファイル，プログラム，ソース・データ収集機能，入力，ユーザ・マシン・インタフェース，処理ステップ，出力は，種々のシステム設計仕様書に一致する事を，新規システム開発と改訂プロジェクトは保証すること
- ・新規システム開発と改訂プロジェクトにおいて，重要な技術的，論理的な矛盾が認識される都度，効果的なシステム設計再評価プロセスを実施するかどうかを決定すること
- ・新規システム開発と改訂プロジェクトでは，技術的な設計上の矛盾，または必要な機能変更が存在するかを判定すること
- ・新規システム開発，改訂プロジェクト，概念的なシステム設計においては，可能な限り早い時期に，入力と出力の正確性/完全性/適時性/正当性（承認）を保証し，さらにセキュリティ概念を設計に組込むことを保証する内部統制とセキュリティ規程の適切性を評価すること
- ・新規システム開発と改訂プロジェクトにおいては，エンド・ユーザに対する可用性と信頼性の改善，および情報サービス部門保守要員の為の保守容易性の改善の観点から設計を評価すること
- ・プロジェクトにおいては，アプリケーション・プログラムのデータ・インティグリティの検証についての妥当性を評価すること
- ・新規システム開発と改訂プロジェクトにおいては，ユーザ参照資料が最新であり，システム文書と一致し，ユーザ・ニーズを充分満足させるものである事を保証すること

以下につき有効性の詳細なレビューを実施：

- ・プログラム仕様作成プロセスは，プログラムがユーザ設計仕様書に準拠して作成されることを保証する
- ・入力仕様作成プロセスは，プログラムがユーザ設計仕様書に準拠して作成されることを保証する
- ・ユーザ・マシン・インタフェース仕様作成プロセスは，プログラムがユーザ設計仕様書に準拠して作成されることを保証する
- ・処理仕様作成プロセスは，プログラムがユーザ設計仕様書に準拠して作成されることを保証する
- ・出力仕様作成プロセスは，プログラムがユーザ設計仕様書に準拠して作成されることを保証する

サンプリングされた新規システム開発と改訂プロジェクトに対して，組織のテスト標準並びに関係するテスト計画の実施について詳細なレビューを実施する

システム，システムについての報告書，ユーザの文書/参照資料，ヘルプ機能などに対するユーザ満足度について詳細なレビューを実施する

► 実証性テストの結果:

新規システム開発，または改訂プロジェクトに使用される組織のシステム開発ライフサイクル方法論の欠陥

ユーザ要件を反映しない設計仕様書

組織のデータ･ディクショナリ規約に準拠しないファイル要件

新規システム開発，または改訂プロジェクトにおいて，次に対する定義が不適切 ：

ファイル，プログラム，ソース･データ選択，入力，ユーザ･マシン･インタフェース，処理，出力，統制能力要件

新規システム開発，または改訂プロジェクトにおいて，設計プロセスで可用性が考慮されなかった

新規システム開発，または改訂プロジェクトにおいて，アプリケーション･プログラム･ソフトウェアにデータ･インティグリティの欠陥

組織のテスト標準の欠陥により，データ処理が正しく行われず，正しくないデータ･レポートが出力されてしまうなどの結果をもたらすシステムの導入

新規システム開発，または改訂プロジェクトにおけるテスト計画の欠陥

新規システム開発，または改訂プロジェクトにおけるユーザの参照資料/支援資料の欠陥

重要な技術上，論理上の矛盾がシステム開発または保守の際に識別されたが，システム設計の再評価は行われず，それ故に修正されなかったか，またはシステムに非効率的，非効果的，非経済的な修正を実施しなければならなかった

AI3 技術基盤の取得と保守

コントロール目標

1 新しいハードウェアとソフトウェアの評価
2 ハードウェアに関する予防保全
3 システム･ソフトウェアのセキュリティ
4 システム･ソフトウェアの導入
5 システム･ソフトウェアの保守
6 システム･ソフトウェアの変更管理

高いレベルと詳細コントロール目標の監査手続

理解

面接対象者:

情報サービス部門の計画策定/運営委員会
情報統括役員
情報サービス部門の上級管理者

収集すべき証拠資料:

ハードウェア並びにソフトウェアの取得，導入，保守に関する方針と手続
上級管理者の運営の役割と責任
ITの目標と長期/短期計画
状況報告書と会議議事録
ベンダのハードウェアとソフトウェアに関する文書
ハードウェアとソフトウェアのレンタル契約書，またはリース契約書

コントロール評価

評価視点:

以下を保証する方針と手続が存在すること:

- ･システム全体の性能に及ぼす影響について新しいハードウェアとソフトウェアを評価する為の正式な評価計画が用意されていること
- ･システム･ソフトウェアをアクセスし，その結果として情報システムの運用環境に介入されてしまうことを制限できること
- ･システム･ソフトウェアの設定，導入，保守により，システム上に格納されているデータやプログラムのセキュリティが危険にさらされないこと
- ･システム上に格納されているデータやプログラムのインティグリティが保証されるように，システム･ソフトウェア･パラメータが設定されること

(評価視点続き)

・技術基盤に関する取得と保守のフレームワークに従って，システム・ソフトウェアが導入され，保守されること
・システム・ソフトウェア・ベンダは，彼らのソフトウェアとそのソフトウェアへのあらゆる修正に対して，インティグリティ保証書を提供すること
・システム・ソフトウェアは本番環境に導入される前に，徹底したテスト（即ち，システム開発ライフサイクル方法論を使用して）を実施すること
・ベンダが用意したシステム・ソフトウェア導入用のパスワードは，導入時に変更され，システム・ソフトウェアの変更は組織の変更管理手続に従って管理されること

性能上の不具合の頻度と影響を減少させる為に，ハードウェア（情報サービス部門と影響を受けるユーザ部門の両方に管理される）予防保守の為の方針と手続が存在すること

情報サービス部門と影響を受けるユーザ部門によって操作される各々のハードウェア機器に対して，ベンダが規定した予防保守に関する処置と保守頻度が守られていること

準拠性評価

準拠性テスト:

すべてのシステム・ソフトウェア（修正もすべて含まれる）に対して，ベンダより与えられるシステム・ソフトウェア・インティグリティ保証書が存在すること，また，システム・ソフトウェアのエクスポージャーについて述べていること

性能評価はシステム要件との比較においてなされること

性能評価の正式な承認プロセスが存在すること

予定されているハードウェア保守は，重要な，または機密度の高いアプリケーションへのいかなるマイナスの影響も与えないことを予防保守スケジュールで保証すること

予定されている保守がピーク業務期間に計画されていないこと，情報サービス部門と影響を受けるユーザ・グループによる運用は，日常予定された予防保守への対応に十分に柔軟であることを保証すること

予定外の保守に対して，想定されるハードウェア・ダウン時間に充分便宜を図るだけの用意があることを，情報サービスの運用スケジュールで保証すること

システム上に格納されているデータとプログラムのインティグリティを保証する為に，適切な情報サービス部門要員によってシステム・ソフトウェア・パラメータが正しく設定されていることを，システム・ソフトウェア・パラメータで保証すること

アクセスが，情報サービス部門内の限定された人数のオペレータのみに制限されていること

システム・ソフトウェアは，技術基盤の取得と保守のフレームワークに従って，導入，保守されていること

本番環境への導入が許可される前に，すべてのシステム・ソフトウェアに対して徹底したテスト（システム開発ライフサイクル方法論を使用して）が行なわれること

ベンダ提供のシステム・ソフトウェア導入用のパスワードは，すべて導入時に変更されていること

すべてのシステム・ソフトウェアに対する変更が，組織の変更管理手続に従って管理されていること

システム管理（例，システムとネットワークへの新規ユーザ追加；データベースの作成とバックアップ；データ・ストレージへのスペース割り当て；システム優先順位；等）が，情報サービス部門内の限定された人数のオペレータのみに制限されていること

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:

ハードウェアとソフトウェアの取得，導入，保守について，類似した組織あるいは適切な国際標準／認められた業界のベスト･プラクティスに対して，ベンチマークを実施すること

以下につき詳細なレビューを実施すること:

- ･正式なハードウェアとソフトウェアの性能要件（トランザクション量，処理と応答の時間，ファイルとデータベースのサイズ，ネットワーク･ボリューム，通信プロトコル互換性の参照を含む）が，システムに対して存在するかどうかを判定する為にサンプリングされた本番システム，システム開発/改訂プロジェクトの文書
- ･ベンダ･ガイドラインに従って保守が行なわれており，それがシステム全体の性能に影響を与えないような方法で計画されているかどうかを判定するためのハードウェア保守実施
- ･システム･ソフトウェアの具備する論理的なセキュリティ･アクセス制限を迂回する潜在的な能力を評価する為のサンプリングされた本番システムと開発中/改訂中のシステム文書
- ･技術基盤並びにシステム･インティグリティに関して，取得と保守のフレームワークへの準拠性が保持されている事を保証するシステム･ソフトウェアの導入，維持，変更管理

► 実証性テストの結果:

システム全体の性能に影響を与えてきた性能評価

システム全体の性能に影響を与えてきた予防保守問題

システム･ソフトウェアの設定，導入，保守時に弱点（不適切なシステム･ソフトウェア･パラメータ設定を含む）があり，その結果システムに格納されているデータとプログラムのセキュリティを危険にさらしてきたこと

システム･ソフトウェアのテスト時に弱点があり，その結果システムに格納されているデータとプログラムのセキュリティを危険にさらしかねないこと

システム･ソフトウェア変更管理プロセスに弱点があり，システムに格納されているデータとプログラムのセキュリティを危険にさらしかねないこと

AI4 IT関連手続の作成と保守

コントロール目標

1 将来の運用要件とサービス水準
2 ユーザ手続マニュアル
3 運用マニュアル
4 教育資料

高いレベルと詳細コントロール目標の監査手続

理解

面接対象者:

情報サービス部門のアプリケーション開発担当者
情報サービス部門の保守担当者
情報サービス部門の変更管理担当者
情報サービス部門の運用担当者
情報サービス部門の人的資源／教育担当者
情報サービス部門の品質保証管理者
情報システム資源のサンプリングされたユーザ

収集すべき証拠資料:

次に関する組織の方針と手続:
戦略上の計画とビジネス目標,
情報システム計画策定とアプリケーション開発
次を含むシステム開発に関連する情報サービス部門の方針と手続:
組織図, システム開発ライフサイクル方法論, キャパシティ・プランニング, ユーザ・マニュアルと運用マニュアル, 教育資料, テストと本番状況への移行, ビジネス再開／危機管理計画文書

コントロール評価

評価視点:

運用上の要件は, パフォーマンス統計履歴の入手, ユーザ入力の増減の予測によって決められること
期待されるサービス水準と性能の想定は, 追跡, 報告, 改善の機会を可能にする為に充分詳細であること
運用上の要件とサービス水準は, 性能履歴, ユーザとの調整, 業界ベンチマークの使用により決定すること
サービス水準と処理要件が, 新規システムの計画における不可欠なステップであること
あらゆる情報システムの開発/導入/改訂プロジェクトの一部として, ユーザ手続マニュアル, 運用マニュアル, 教育資料が作成され, 最新の状態に更新されていること

準拠性評価

► 準拠性テスト:

運用上の要件が適切で，運用面並びにユーザの期待を反映していること
運用上の性能が測定され，伝達され，不備な点は訂正されていること
運用要員とユーザが，性能要件を意識していること
運用要員は，自己責任の範囲内ですべてのシステムと処理に関する運用マニュアルを所持すること
アプリケーション開発から本番へのいかなるプログラムの移行に際しても，運用マニュアルの更新あるいは新規作成が要求されていること
ユーザ教育マニュアルが，すべてのアプリケーションに対して存在し，アプリケーションの現在の機能性を反映していること
すべての現行システム，新規システムに対して教育マニュアルがあり，それらはユーザにとって満足いくものであり，日常業務における実際のシステムの利用法を反映していること
ユーザ・マニュアルは以下の内容を含むが，それに限定はされない：
- ・システムと環境の概要
- ・全システムの入力/プログラム/出力/他システムとの結合に関する説明
- ・すべてのデータ入力画面とデータ表示画面に関する説明
- ・すべてのエラー・メッセージと適切な応答に関する説明
- ・問題の上申手続きと資源

オペレータ・マニュアルは，以下の内容を含むが，それに限定はされない：
- ・システム名称，プログラム名称，実行順序
- ・入力，処理，出力されるすべてのファイル名称とメディア・フォーマットの定義
- ・日次，週次，月次，四半期毎，年度末などの実行予定
- ・オペレータによる入力を必要とするコンソール・コマンドとパラメータ
- ・コンソール・エラー・メッセージと応答
- ・諸々の時点，または異常終了の際のバックアップ，リスタート，リストア手続
- ・特別な出力形式あるいは手続；レポート/出力の配付
- ・もし適切であるならば，緊急修正手続

アプリケーション文書，ユーザ・マニュアルと運用マニュアルについて継続的な保守と教育が行われていること

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:

サンプリングされたシステム開発プロジェクトに対して，以下に関するドキュメンテーションの評価と承認を行うこと
- ・ユーザに関し，将来の要件とサービス水準を考慮すること
- ・ユーザ・マニュアルの作成と維持に関する作業と配付
- ・運用マニュアルの作成と維持に関する作業と配付
- ・新規システムあるいは新たに改訂されたシステムを理解し，使用する為のユーザ教育に関する作業と配付

(実証性テスト続き)

マニュアルが作成され，教育が提供されている点も含め，システム開発成果が十分であるかを確かめる為にユーザ･インタビューを実施すること

ユーザ･マニュアルと運用マニュアルが，常に最新状態に維持されているかを分析すること

► 実証性テストの結果:

ユーザ･マニュアル，運用マニュアル，教育マニュアルの欠陥

以下の両者間でサービス水準について同意がなされなかったこと

- ･ベンダと情報サービス部門
- ･情報サービス部門とユーザ
- ･組織が要求されているアプリケーションを開発し，稼働させる点に弱点を持つこと

AI5 システムの認証と導入

コントロール目標
1 教育
2 性能最適化の適用
3 移行
4 変更テスト
5 並行／パイロットテストの基準と性能
6 最終検収テスト
7 セキュリティテストと認証
8 運用テスト
9 本番への移行
10 ユーザ要件の適合度評価
11 管理者による導入後レビュー

高いレベルと詳細コントロール目標の監査手続

面接対象者:

情報統轄役員
情報サービス部門の管理者
情報サービス部門の教育/アプリケーション開発/セキュリティ/品質保証/運用の管理者
セキュリティ管理者
新規開発/開発中のシステムに対しサンプリングされたユーザ管理者
システム開発資源に関するベンダとの契約書

収集すべき証拠資料:

システム開発ライフサイクルの計画策定に関する組織体の方針と手続，並びに次に関わる情報サービス部門の方針と手続 ：
セキュリティの方針と委員会;システム開発ライフサイクルの計画策定;プログラム･テスト/ユニット･テスト/システム･テストの計画に関するシステム開発テスト手続;ユーザ教育;テストから本番へのシステム移行，品質保証，教育
システム開発ライフサイクル計画とスケジュール，変更依頼プロセスを含むシステム開発ライフ･サイクル･プログラミング標準
サンプリングされたシステム開発結果の状況報告書
以前の開発結果の導入後報告書

コントロール評価

► 評価視点:

システム開発ライフサイクル･プロセスに関する方針と手続が存在すること
正式なシステム開発ライフサイクル方法論が，以下についてのフェーズ化されたアプローチも含めて，但しそれに制約されないが，関するシステムの導入と承認に関して適切であること ：
　　教育，性能見積り，移行計画，プログラム･テスト，ユニット（プログラムのグループ）･テスト，全体システム･テスト，並行/プロトタイプ･テスト計画，検収テスト，セキュリティ･テストと承認，運用テスト，変更管理，導入/導入後のレビューと修正
開発取組みの中の一部としてユーザ教育が行われていること
プログラム/システム管理が，組織のセキュリティ標準，並びに情報サービス部門の方針，手続，標準に準拠していること
開発中のシステムに関しては，種々の開発/テスト/本番用のライブラリーが存在すること
テストの成功/失敗/再試行の終了に関する判定は，事前に決定された基準に依ること
品質保証プロセスは，開発から本番ライブラリーへの独立性を保持した移行，必要とされるユーザと運用グループによる検収の完全性を含むこと
ボリューム/処理間隔/出力の可用性のシミュレーションに関するテスト計画，導入と承認はプロセスの一部であること
幾つかのシステム開発への取組みをサンプリングし，関連する教育プログラムには以下が含まれること：
　　前システムとの差異，変更が次に及ぼす影響――入力，収集，処理，スケジューリング，配付，他システムとのインタフェース，エラーとエラーの解決
自動化ツールが，開発されたシステムを最適化し，本番ではこれらのツールは効率性を求めて使用されること
パフォーマンスが最適でない場合は，その問題解決に取り組んでいること

準拠性評価

► 準拠性テスト:

すべての新規システム開発の取組みには，正式なユーザ教育計画が含まれていること
すべての開発に関わる導入，実施に関しては，正式なシステム開発コントロールとユーザ教育が必要である事をスタッフが認識し，理解していること
ユーザをサンプリングし，彼らが，システム設計，承認，テスト，教育，移行，導入プロセスについて責任を自覚し理解していること
新規，あるいは改訂システムについて，システムの実コスト対見積コスト，実際の性能対期待された性能が追跡されていること
下記のような情報システム資源の全領域をカバーするテスト計画が存在すること：
　　アプリケーション･ソフトウェア，施設，技術，およびユーザ

(準拠性テスト続き)

以下も含めて，システム開発の全フェーズと責任をユーザが理解していること：
- ・開発サイクルの間の反復を含む設計仕様書
- ・コスト対効果の分析と実現可能性の調査
- ・システム開発プロセスの各ステップで必要とされる承認
- ・テスト計画とその都度のテスト結果への掛かり合いと評価
- ・開発サイクル中でのシステムの承認と検収
- ・システムの最終承認と検収
- ・最近引き渡されたシステムに対し行われた教育が十分であることの評価

開発スタッフと管理者は，一旦同意されたユーザ要件の安定性を確かめること
顧客満足度を，自社開発とベンダによる成果物とで比較すること

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:

システムの導入と承認に関して，類似した組織または適切な国際標準／認められた業界のベスト・プラクティスとのベンチマークの実施
以下にあげるものの詳細なレビュー：
- ・最終期限を守り，かつ完成時のシステム機能性も含めて顧客が満足している作業を行っている開発グループ
- ・以前のシステムに関連する教育資料
- ・品質保証部門による，独立したレビュー，およびシステムのテストから本番環境と本番ライブラリーへの移行
- ・保守と最適化の為の統計値を収集するのに使われ，かつ最小のコストで最大の性能を得る目的で開発されたアプリケーションに対するサポートを保証するネットワークと資源の監視ツール
- ・以下の有効性を決める開発の取り組みについての記録：
  - ・ユーザ教育
  - ・セキュリティ
  - ・ソフトウェア性能
  - ・テスト文書と結果
  - ・移行計画
  - ・本番への移行
  - ・開発時の変更管理
  - ・ユーザのニーズ満足度
  - ・並行テスト，またはパイロット・テスト
  - ・導入後レビュー
- ・システム設計プロセスに関する内部監査，または外部監査の監査結果
- ・テスト結果が事前に定義された基準を満たし，テスト計画はシステムのすべての機能を網羅している事を確認する為のテスト結果
- ・テスト結果/あらゆる打ち切られたテスト/開発プロジェクトについての管理者の討議

(実証性テスト続き)

- 開発プロセスへのユーザの参加
- 必要に応じ，アクティビティやエラー分析の再現に必要な監査証跡
- 以下を含む開発の取り組みへのベンダの参加 ：
  - コストの合理性
  - 最終期限の厳守性
  - 実現された機能性

► 実証性テストの結果:

サンプリングされた最近のシステム開発ライフサイクル・プロジェクトに対して：

- システム開発プロセスの各フェーズでのユーザの参加と正式な承認
- プログラム/ユニット/システム（並行，あるいはプロトタイプを含む）/移行/導入の各々に関するテスト計画，および導入後のレビュー
- セキュリティと内部統制標準への適切な一貫性保持
- 適切なデータ移行に関する作業とスケジュール
- システムの開発，改訂，保守から独立したテストの実施
- システムの機能性，セキュリティ，インティグリィティ，残存リスクに関するユーザによる正式な承認

スケジューリング，実行，リストア/リスタート，バックアップ/バックアウト，およびエラー解決の為の運用マニュアルが以下のことに言及していること：

- 本番ライブラリーの開発およびテスト用ライブラリーからの物理的かつ論理的な分離
- ユーザの期待するものと提供されたシステムの機能性との間で矛盾が生じたときの解決手続

ベンダに対して：

- ベンダとの関係が正式なものであり，契約書が存在すること
- 明確なサービスとコストについての要点が述べられていること
- ベンダの業績が，組織のシステム開発ライフサイクル方法論を使用して平等に管理されていること
- ベンダが契約通りに性能，期限，コスト明細を遵守してきたこと

AI6 変更管理

コントロール目標
1 変更要求の開始とコントロール 2 影響の評価 3 変更の管理 4 文書化と手続 5 権限付与された保守の承認 6 ソフトウェアのリリース方針 7 ソフトウェアの配付

高いレベルと詳細コントロール目標の監査手続

理解

面接対象者:

情報統轄役員
情報サービス部門の管理者
情報サービス部門のシステム開発/変更管理品質保証/運用/セキュリティの管理者
情報システム・アプリケーションの設計と使用に関わるサンプリングされたユーザ部門管理者

収集すべき証拠資料:

以下に関する組織の方針と手続 :
情報システムの計画策定, 変更管理, セキュリティ, システム開発ライフサイクル
以下に関する情報サービス部門の方針と手続 :
正式なシステム開発ライフサイクル方法論, セキュリティ標準, テスト標準, 独立した品質保証, 導入, 配付, 保守, 緊急時変更, ソフトウェアのリリース, システムのバージョン管理
アプリケーション開発計画
変更管理要求フォームと記録
アプリケーション開発サービスに関するベンダ契約

コントロール評価

評価視点:

ユーザからのシステム変更要求を優先順位付けする為の方法論が存在し, 使用されていること
緊急時変更手続が運用マニュアルに記述されていること
変更管理は, ユーザと開発グループの両者に対する正式な手続であること
変更管理記録は, 示されているすべての変更が解決されていることを保証すること

(評価視点続き)

ユーザが変更要求に対するターンアラウンド即ち適時性とコストに満足していること
サンプリングされた変更管理記録上の変更に対して：
- その変更により，プログラムと運用ドキュメンテーションも変更されていること
- 変更が文書化を伴っていること
- 現在のドキュメンテーションが変更された環境を反映していること

変更プロセスを監視し続け，承認，対応時間，対応の有効性，そのプロセスに関する顧客満足度等の改善をはかること
構内自動電話交換機（PBX）システムの維持は，変更管理手続きに含まれること

準拠性評価

準拠性テスト:

サンプリングされた変更に関して，以下のことが管理者により承認されてきていること：
- 変更要求
- 変更仕様書
- ソース・プログラムへのアクセス
- プログラマーによる変更完了
- テスト環境へのソース移動要求
- 検収テストの完了
- コンパイルと本番への移行要求
- 全体的なかつ特定されたセキュリティへの影響が判定され，承認されていること
- 配付プロセスが作成されていること

以下に関する変更管理文書についてのレビュー：
- 変更の依頼日付
- 依頼人
- 変更依頼の承認
- 行われた変更の承認 — 情報サービス部門
- 行われた変更の承認 — ユーザ
- 文書更新日付
- 本番への移行日付
- 変更に関する品質保証承認
- 運用部門による承認

傾向を識別するために，システムへなされた変更のタイプを分析すること
情報サービス部門のライブラリーの適切性を評価し，エラー回帰を防止する為にベースライン・コードのレベルの存在を決定すること
変更に関して，コードのチェック・イン/チェック・アウトの手続きが存在すること
記録された変更要求はすべて顧客の満足のいくように解決されており，記録されずに実施された変更は一切ないことを変更管理記録で保証すること
ユーザは正式な変更管理手続の必要性を認識し，理解していること
スタッフの強制プロセスが，変更管理手続への準拠を保証すること

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:

変更管理管理者に関して，類似した組織または適切な国際標準/認められた業界のベスト・プラクティスとのベンチマークを実施すること

サンプリングされた情報サービス部門のシステムに対して：

- ・変更依頼またはシステム変更が，影響を受けるユーザ部門やサービス・プロバイダの管理者によって承認され，優先順位が付けられていることを文書を見て判別できること
- ・変更管理フォーム上で影響評価が適切になされていることを確認できること
- ・システム・サービス機能が，変更依頼票の受領を承認していること
- ・変更に対して適切な開発資源を割当てていること
- ・システム・テスト並びにユーザ・テストの計画と結果が適切であること
- ・テストから本番への正式の移行は，品質保証グループを介して実施していること
- ・ユーザ・マニュアルと運用マニュアルは，変更を反映し更新されていること
- ・新しいバージョンが，適切なユーザへ配付されていること

► 実証性テストの結果:

サンプリングされたシステム変更に関して：

- ・承認された変更だけが行われている
- ・すべての変更が説明されている
- ・現行ライブラリー（ソースとオブジェクト）が最新の変更を反映している
- ・以下にあげる二者間での変更管理手続の相違が記録され説明されている：
  - ・購入アプリケーションと内製アプリケーション
  - ・アプリケーション・ソフトウェアとシステム・ソフトウェア
  - ・変更管理に対するベンダの扱い方

デリバリとサポート

DS1 サービスレベルの定義

コントロール目標

1 サービスレベル合意書のフレームワーク
2 サービスレベル合意書の内容
3 性能手続
4 モニタリングと報告
5 サービスレベル合意書と契約書のレビュー
6 課金項目
7 サービス向上プログラム

高レベルかつ詳細なコントロール目標の監査

理解

面接対象者:

情報統括役員 (CIO)
情報サービス担当の上級管理者
情報サービス契約／サービスレベルの管理者
情報サービス運用の管理者
ユーザの管理者

収集すべき証拠資料:

ベンダユーザの関係に関する組織全体の方針と処理手順
以下に関する情報サービス機能の方針と処理手順
- サービスレベルの合意書
- 運用報告書の内容, 報告時期, および配付
- パフォーマンスの測定方法
- 調整行動の活動内容

以下に関する情報サービス部門の文書
- サービスレベルに関するパフォーマンス報告書
- 課金を計算するためのチャージバックアルゴリズムと方法論
- サービス向上のためのプログラム
- パフォーマンス不達成時の求償
- 内外の利用者とベンダとのサービスレベル同意書

コントロール評価

評価視点:

サービスレベル同意書の締結プロセスが, 方針として定められている

(評価視点続き)

プロセスにおけるユーザの参画が，同意書の作成と改訂において要求されている
ユーザとベンダの責任が定義されている
管理者が，特定のサービスパフォーマンス基準の達成状況と遭遇したすべての問題についてモニタリングし報告している
管理者による通常のレビュー手順が存在している
パフォーマンス不達成時の求償過程が確認されている
サービスレベル同意書に以下のものが含まれている (ただし，それに限定されていない)

- ·サービスの定義
- ·サービスのコスト
- ·定量化可能な最低限のサービスレベル
- ·情報サービス部門から得られるサポートレベル
- ·可用性，信頼性，拡張余力
- ·継続性計画
- ·セキュリティ要件
- ·同意書の内容を改訂する際の手続
- ·サービスについてのプロバイダとユーザ間での文書化された公式な合意書に関する記述
- ·有効期間と，新たな期間に向けてのレビュー／更新／非更新
- ·実績報告の内容とその頻度，およびサービスに対する支払
- ·料金が過去の実績，業界，慣例と比較して現実的であること
- ·課金の計算方法
- ·サービス向上のコミットメント

準拠性評価

► 準拠性テスト:

過去および進行中のサービスレベル同意書の事例。以下のものが含まれる。

- ·サービスの定義
- ·サービスのコスト
- ·定量化可能な最低限のサービスレベル
- ·情報サービス部門から得られるサポートレベル
- ·可用性，信頼性，拡張余力
- ·同意書のすべての内容を改訂する際の手続
- ·継続性計画
- ·セキュリティ要件
- ·サービスに関するプロバイダとユーザとの文書化された公式の承認を得た同意書
- ·有効期間と，新たな期間に向けてのレビュー／更新／非更新
- ·実績報告の内容とその頻度，およびサービスに対する支払
- ·料金が過去の実績，業界，最適実務と比較して現実的であること
- ·課金の計算方法
- ·サービス向上のコミットメント
- ·ユーザとプロバイダの公式の承認

(準拠性テスト続き)

適切なユーザがサービスレベル同意書に関する手順と手続について知り，理解している
現行のサービスレベルの手順と現在の同意書に関するユーザの満足レベルが，十分である
サービスにおいて，パフォーマンス不達成の確かな理由および適切なパフォーマンス向上プログ ラムを保証する記録が提供されている
現在の課金の正確性が，同意書の内容に適合している
サービス向上に関して先に得られたコミットメントに関するパフォーマンスの履歴が証跡としてのこされている
特定のサービスパフォーマンスの達成についての報告が，満足のいくパフォーマンスを保証するために，管理者によって適切に利用されている
遭遇したすべての問題についての報告が，正しい対応を行うことを保証するために，管理者によって適切に利用されている

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:

同様の組織や適切な国際標準あるいは産業界でよく知られた最適実務と対比してサービスレベル合意書の判断基準を決める (ベンチマーキング)
以下についてレビューする:
- ・サービスレベル合意書において，契約事項が定義され守られているかを確認するために定性的かつ定量的な規定が決められているか
- ・選定されたサービスレベル合意書において，問題，特にパフォーマンス不達成に対する問題解決手続が記載され守られているか

► 実証性テストの結果:

情報サービスのプロバイダとユーザの関係に関する記述や調整や意見交換が適切になされていること
選択された情報のカテゴリの計算の正確さ
サービスレベルの報告をうけて管理者が進めているレビューおよび調整活動
提案されているサービス向上が，コスト効果分析からみて適切であること
将来のサービス向上に関する公約に対してプロバイダの能力が適切であること

DS2 第三者機関のサービスの管理

コントロール目標
1 供給者とのインタフェース 2 オーナとの関係 3 第三者機関との契約書 4 第三者機関の適格性 5 アウトソーシング契約書 6 サービスの継続 7 セキュリティとの関係 8 モニタリング

高レベルかつ詳細な コントロール目標の監査手続

理解

► **面接対象者:**

情報統括役員 (CIO)
情報サービス担当の上級管理者
情報サービス契約／サービスレベルの管理者
情報サービス運用の管理者
情報サービスのセキュリティ担当者

► **収集すべき証拠資料:**

サービスの購入，特に第三者機関ベンダとの関係に関する組織全体としての方針と手続
以下に関する情報サービス機能の方針：第三者機関との関係,ベンダの選択手続,そのような関係における契約内容,物理的および論理的セキュリティ,ベンダの品質維持,コンティンジェンシー計画,アウトソーシング
現在のすべての第三者機関との関係およびその各々についての現在の契約のリスト
第三者機関との関係およびサービスに関するサービスレベル報告
契約のレビュー，パフォーマンス評価，および第三者機関管理について議論したミーティングの議事録
すべての第三者機関に対する守秘契約
ベンダにとって利用可能なプロファイルと資源のセキュリティアクセスのリスト

コントロール評価

► **評価視点:**

第三者機関に関する情報サービス機能の方針と手続が存在し，組織の一般的な方針と整合性を持っている

(評価視点続き)

契約，契約の内容についての定義，契約締結にあたってのオーナまたは交渉担当の管理者について，明確に定められた方針が作成され，維持され，モニタリングされ，必要に応じて再調整されている
プロジェクトの実行に係わる独立したエージェントや例えば下請け業者のような他の業者との間のインタフェースが定義されている
契約が，第三者機関のサプライヤとの関係について十分かつ完全な記録をあらわしている
サービスの継続性についての契約が明確に定めれれており，これらの契約に，ユーザへのサービスの継続を保証するためにベンダが作成したコンティンジェンシー計画が含まれている
契約には少なくとも以下が含まれている

- 公式の経営者と法的な承認
- サービスを提供する法人格
- 提供されるサービス
- 定性的および定量的なサービスレベル同意書
- サービスのコストとサービスへの支払いの頻度
- 問題解決の過程
- パフォーマンス不達成時の求償
- 契約解消過程
- 契約改訂過程
- サービスに関する報告－内容，頻度，配付
- 契約の有効期間における契約当事者間の役割
- ベンダが提供するサービスの継続の保証
- サービス利用者とプロバイダとのコミュニケーションの手順と頻度
- ベンダに提供されるアクセスのレベル
- セキュリティ要件
- 非開示の保証
- アクセスの権利と監査の権利

適切な場所で条件付き捺印証書の合意に関して交渉が行われている
潜在的な第三者機関を評価する際に，要求されたサービスを提供する能力を評価基準に従って適切に評価している (当然の注意事項)

準拠性評価

準拠性テスト:

契約のリストと現在の契約が正確である
契約のリストにないベンダは何らのサービスも提供していない
契約にあるプロバイダが，規定されたサービスを実際に提供している
プロバイダの管理者／オーナが契約で定めたその責任を理解している
第三者機関に関する情報サービス機能の方針と手続が存在し，組織の一般的な方針と整合性を持っている
契約，契約の内容についての定義，契約締結にあたってのオーナまたは交渉担当の管理者について，明確に定められた方針が作成され，維持され，モニタリングされ，必要に応じて再調整されている

(準拠性テスト続き)

契約が，第三者機関のサプライヤとの関係について十分かつ完全な記録をあらわしている
サービスの継続性についての契約が明確に定めれれており，これらの契約に，ユーザへのサービスの継続を保証するためにベンダが作成したコンティンジェンシー計画が含まれている
契約には少なくとも以下が含まれている
- ・公式の経営者と法的な承認
- ・サービスを提供する法人格
- ・提供されるサービス
- ・定性的および定量的なサービスレベル同意書
- ・サービスのコストとサービスへの支払いの頻度
- ・問題処理の解決
- ・パフォーマンス不達成時の罰金
- ・契約解消の手順
- ・契約改訂の手順
- ・サービスに関する報告－内容，頻度，配付
- ・契約の有効期間における契約当事者間の役割

ベンダが提供するサービスの継続の保証
- ・サービス利用者とプロバイダとのコミュニケーションの手順と頻度
- ・契約の有効期間
- ・ベンダに提供されるアクセスのレベル
- ・セキュリティ要件
- ・非開示の保証
- ・アクセスの権利と監査の権利

ユーザが，サービス提供の契約方針と契約そのものの必要性を知り，理解しているベンダと現行の組織との間の適切な独立性
ベンダの探索と選別の手順の独立性がある
セキュリティアクセスリストに必要に応じた最小限のベンダ社員の数が含まれており，そのアクセスが必要最小限にとどまるものである
組織の資源にアクセスするハードウェアとソフトウェアが，ベンダによる利用を最小にするよう管理されコントロールされている
提供されている実際のサービスレベルが，契約上の義務に比較して高い
アウトソーシングの設備，社員，運用，およびコントロールが，期待と比較可能なパフォーマンスの要求レベルを保証している
第三者機関によるサービス提供の継続的なモニタリングが，管理者によって実行されている
契約部門の業務に対する外部監査が行われている
要求されたサービスを提供する能力について潜在的な第三者機関を評価した評価報告書がある
過去および現在の法廷活動行為が記録されている
プロジェクトの管理に係わる外部代理人との連携事項がが契約書に記されている
PBXの販売業者との契約がなされている

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:

サービスレベル同意書について，同様の組織または適切な国際的な標準／産業内のよく知られた最適実務に対して行われたベンチマーキング

義務を確認する定量的および定性的な条項を決定するための各々の第三者機関契約の詳細なレビューが定義されている

►実証性テストの結果:

情報サービスについてのプロバイダとユーザの関係について，記述され，調整され，意見交 換された規定

選択された契約にあるサービスに正確に課金されたことをあらわす第三者機関の請求書

第三者機関のベンダを担当する組織の連絡部門が，第三者機関とサービスのユーザとの間における契約上の問題に関する意見交換を保証している

合法的な委員会と管理者がすべての契約を承認している

進行中のリスクアセスメントが，関係の必要性または関係の修正の必要性を確認するために行われている

契約の報告についての管理者の進行中のレビューと訂正行動が行われている

パフォーマンスを比較することが可能な様々な内外および産業と，課金についての合理的な比較が行われている

コンティンジェンシー計画が，契約されたすべてのサービス，特に情報サービス機能の障害回復サービスについて，適切に作成されている

アウトソースした機能について，パフォーマンス向上やコスト削減をすべき明白な欠点や機会が存在している

契約管理部門の独立した監査を含む勧告の実施が行われている

DS3 性能とキャパシティの管理

コントロール目標
1 可用性と性能要件 2 可用性の計画 3 モニタリングと報告 4 モデリング･ツール 5 積極的な性能管理 6 負荷の予測 7 資源のキャパシティ管理 8 資源の可用性 9 資源のスケジュール

高レベルかつ詳細な コントロール目標の監査手続

理解

面接対象者:

情報サービス担当の上級管理者
情報サービス担当の運用管理者
情報サービス担当のキャパシティ管理者
情報サービス担当のネットワーク管理者

収集すべき証拠資料:

可用性，パフォーマンス･モニタリングと報告，作業量予測，キャオパシティ管理，およびスケジュール作成に関する組織全体の方針と処理手順
組織の業務計画への結合，サービスの可用性，可用性の計画，継続的なモニタリングとパフォーマンス管理に関する情報サービス機能の方針と処理手順
キャパシティとパフォーマンスを考慮したベンダ製品の言明
ハードウェア，ソフトウェア，通信，および周辺機器の製品の現在のすべての第三者機関のリスト
通信ネットワークのモニタリング報告
キャパシティ計画，パフォーマンス予想，およびパフォーマンスの「細かなチューニング」について議論したミーティングの議事録
可用性，キャパシティ，作業量，および資源計画の文書
キャパシティとパフォーマンスに関する仮定を含むIT年度予算
問題報告と解決の履歴を含む，情報サービス機能の運用パフォーマンスに関する報告

コントロール評価

► 評価視点:

情報サービス機能により提供されるすべてのサービスについて，タイム･フレームとサービス･レベルが定義されている。
タイム･フレームとサービス･レベルが利用者要件を反映している。
タイム･フレームとサービス･レベルが，装置の潜在的に可能なパフォーマンス予測と整合性を有している。
可用性計画が存在し，現行のものとなっており，利用者要件を反映している。
管理者により指摘されているパフォーマンスの不足について，すべての装置とキャパシティについての継続的なパフォーマンス･モニタリングが行われ，報告されており，また，パフォーマンスの改善の機会について公式に取組みが行われている。
最適な構成のパフォーマンスが，キャパシティを要求されるレベルへ最少化するとともに，パフォーマンスを最大化するようなモデリング･ツールでモニタリングされている。
利用者と運用面のパフォーマンス･グループがともに，キャパシティとパフォーマンスのレビューを積極的に行い，作業量［負荷］スケジュールの修正が行われている。
作業量予想に，変更要求に関する利用者からの入力と，新技術または現行製品の拡張ニ「関するサプライヤからの入力が，含まれている。

準拠性評価

► 準拠性テスト:

パフォーマンス，キャパシティ，可用性報告にある統計が正確で，その中には，予実比較やパフォーマンスの差異についての説明が含まれている。
可用性，キャパシティ，作業量計画の各文書の修正を行う変更手順が，変更に関する技術や利用者要件を反映している。
ワークフロー分析報告が，プロセスの効率をより高める機会について述べている。
利用度合いや可用性に関する利用者向けのパフォーマンス情報報告書が存在し，その中にキャパシティ，作業量のスケジュールおよび傾向の情報が含まれている。
段階的な拡張の手続が存在し，遵守され，問題解決のために適切であること。/
システム開発方法論の導入後フェーズに，将来の成長を決定し，パフォーマンス予測を変更する規準が含まれている。
情報サービス機能により提供される支援のレベルが，組織の目標の実現を支援するのに十分である。

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:

同様の組織や適切な国際標準／産業界でよく知られている最適実務に対比したパフォーマンスとキャパシティの管理の基準（ベンチマーキング）

(実証性テスト続き)

現在実施中のビジネスのニーズのテスト。これによりITの利用期間や 要件がニーズを適切に反映していることを保証する。
キャパシティと資源の計画プロセスのレビュー。これによりビジネスのニーズの変更に基づいて計画が適時，修正されることを保証する。
パフォーマンスの期待値がキャパシティやレスポンスや可用性に関し十分な値であることを確認
コスト／利益分析の観点からパフォーマンス要件を比較。これによりキャパシティまたは資源に多すぎる部分がないことを保証する。
パフォーマンス報告書が作成され，管理者によって定期的にレビューされていることの確認

►実証性テストの結果:

改善の機会や弱点の解決ためのパフォーマンス報告
確認したパフォーマンス予測が利用者の期待に適うものであり，変更要求の基づく修正が計画に反映されていること
処理中に発生した問題が適時記録され，解決のための適切な措置がとられていたことを確認するための，問題のログや報告
発生した特別の問題と，問題解決手順の効果の確認

DS4 継続的サービスの保証

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報サービス担当の上級管理者
情報サービス担当の運用管理者
情報サービス機能継続担当の管理者
人的資源または訓練担当の管理者
情報サービスの継続を必要とする利用者組織
ベンダの回復サイトの管理者
オフサイト保管の管理者
リスク／保険担当の管理者

収集すべき証拠資料:

IT継続性計画のプロセスに関する組織全体の方針と処理手順
次の項目に関連する情報サービス部門の方針と処理手順:IT継続性のフレームワーク, 計画, 観点, 戦略, アプリケーションの優先度付け, 計画のテスト,
通常のバックアップとローテーション, および訓練
IT継続性計画に関する情報サービス部門の方針と処理手順
IT継続性計画のサービスを受ける利用者
IT継続性と利用者が計画するビジネス再開に関する最近のテスト結果
回復が必要な事象が発生したときにアプリケーションの優先順位を決定する方法論
IT継続性の支援サービスを提供するベンダとの契約
ビジネス中断のための保険に関する方針

► 評価視点:

組織全体の方針として，情報サービス部門とIT資源に依存しているすべての組織の両方に対して，IT継続のフレームワークと計画を通常の運用上の要件の一部とすることを要求している。
情報サービス部門の方針と手続において，以下のことを要求している。

- IT継続性計画の開発に関連した一貫性をもつ考え方とフレームワーク
- 回復と復帰の適時性を考慮したアプリケーションの優先順位付け
- 資源の利用者と同様に情報サービス部門にとっての，継続の状況におけるビジネスのロスを考慮したリスク評価と保険
- 特別のテスト，維持，および修正の要件に関する継続性計画を考慮した，特別の役割と責務の概要
- 実際の必要性に先立って，バックアップ・サイトの機器または関連を含む，障害の事象に応じたサービスを提供するための，ベンダとの公式の契約に関する調整
- 各々の継続性計画における最低限の内容が以下の点を含んでいる。
  - すべての関連する職員の安全を保証する緊急時の手続
  - 情報システムサービス部門，障害回復サービスを提供するベンダ，サービスを受ける利用者，および管理者の役割と責務
  - IT継続のための長期的な計画と一貫性を持った障害回復のフレームワーク
  - 代替物（ハードウェア，周辺機器，ソフトウェア）を要するシステム資源のリスト
  - 回復時間と期待されるパフォーマンス基準より求められる，アプリケーションの優先順位の最高位から最低位までのリスト
  - 障害復旧が必要な事象に応じた利益，支払，外部との通信，コスト・トラッキングなどと同様の，コミュニケーションや支援サービスの提供のための管理機能
  - 能力やレスポンスの全体の喪失が最少のものから，各々の段階毎の実行に十分な詳細までの様々な障害のシナリオ
  - 特定の装置と備品について，高速プリンタ，サイン，フォーム，通信装置，電話などやの必要性なものとして識別され，情報資源および代替情報資源が，定義されている。
  - 継続性計画における個人と集団の訓練と周知徹底
  - テスト・スケジュール，直近のテスト結果，および定性の行動が，それ以前のテストに基づいている。
  - 契約したサービス・プロバイダ，サービス，および期待されるレスポンスの列挙
  - 回復のためのOS，アプリケーション，データ・ファイル，操作マニュアル，およびプログラム／システム／利用者の各文書のためのバックアップ・サイトを含む，中心となる資源の所在地に関するロジスティクス情報
  - 中心となる職員の現在の，名前，住所，電話／ポケットベルの番号
  - すべてのシステム資源のオリジナルの所在地での再リカバリのために，再構築の計画が含まれている。
  - 情報システム資源が利用可能となった際に代替的な作業場所を定めるための，すべての利用者にとっての業務の代替。すなわち，代替サイトにおけるシステムは回復しているが，利用者の建物が全焼して利用不可能となっている場合。

(評価視点続き)

継続性計画が考慮すべき規制機関の要件に適合している。
利用者の継続性計画が，重要な処理（手作業やコンピュータ処理）を実行するための物理的な資源の利用不可能性に基づいて作成されている。
電話システム，ボイスメール，FAX，イメージシステムが継続性計画の一部に取り込まれているマイクロフィルムや大容量記憶メディアだけでなくイメージシステム，FAXシステム，紙のドキュメントが継続性計画の一部に取り込まれている

► 準拠性テスト:

継続性計画が存在し，現在用いられており，すべての関連する集団によって理解されている。
通常の継続性計画の訓練が，関連するすべての集団に対して行われている。
計画作成に関するすべての方針と手続が遵守されて行われている。
計画の内容が，上記の記述に基づいた内容となっており，以下の点を含んでいる。

- 継続性計画の目的が適合している。
- 適当な個人が，リーダシップの役割を果たすよう選抜されている。
- 計画が，管理者による適切なレビューと承認を得ている。
- 計画が，最近テストされており，計画通りに行ったかあるいは，発見された欠陥により計画の修正がされている。
- 継続性計画と組織の業務計画が連携している。
- 代替的な手作業の手続が，文書化され，全体テストの一部としてテストされている。

利用者と情報システム機能のスタッフの訓練と周知徹底が，計画にある特定の役割，タスク，および責任について行われ，涵養されている。
契約したベンダとの関係とリード・タイムが，利用者の期待や必要性と一貫性をもっている。
バックアップ・サイトの内容が，通常のオフサイトの交代手続に関連して現行のものとなっており，かつ十分である。

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:

継続性計画について，同様の組織または適切な国際的な標準／よく知られた最適実務に対して行われたベンチマーキング
以下に関する詳細なレビュー：

- 適切な戦略と，全体的な業務上のコンティンジェンシー計画とのインタフェースとを保証する計画目的
- 計画の調整担当者としてリーダシップを発揮すべき責任に関して理解している，適切な担当者
- 上級管理者の適切なレベルによってレビューされ，承認された計画
- 継続性計画に業務上の必要性が含まれている事を確認するため，情報サービス機能と利用者部門から選択されたメンバ

(実証性テスト続き)

- 障害が発生してから処理操作が回復可能になるまでの間に使用することとなった時に利用する代替的な手作業でのデータ処理の利用者手続が，ユーザ部門によって文書化されていること
- オスサイトの所在地において十分な在庫がある事が保証された，アプリケーション固有の備品プライ (すなわち，磁気テープ，伝票の在庫，在庫の証明書等)

►実証性テストの結果:

備品を得るためのリード・タイムと，サービス，タイミング，サービス・レベルおよびコストについての十分な詳細を確認するためのベンダとの契約
特別な通信またはネットワーク構成機器の調達のための取り決め
短期から永久的な業務途絶までの，計画の一部としての様々なシナリオ
利用者の期待と一貫性をもって行われたアプリケーションの優先度付け
オフサイトの必要性に応じたコンピュータ機器に関して文書化された契約が存在すること。
代替サイトの，利用者要件を満足する処理速度，レスポンス，可用性，支援
復旧が必要になった場合のサービスの継続性を保証するベンダの継続性計画
同時障害復旧発生の可能性を削除するための，自サイトから代替サービスプロバイダまでの距離
計画の定期的なテストが行われていること，およびテストに基づいて計画が調整されていること
情報サービス部門の職員も利用部門の職員も継続性計画の訓練を通常受けていること
同様の再構築チーム，タスクおよび責任，そして，代替処理から当初の所在地へ処理を移行するためのテストが存在すること

DS5 システムセキュリティの保証

1 セキュリティ対策の管理
2 識別，認証とアクセス
3 データへのオンライン・アクセスのセキュリティ
4 ユーザアカウントの管理
5 ユーザアカウントの管理者レビュー
6 ユーザアカウントのユーザコントロール
7 セキュリティ監視
8 データ分類
9 識別とアクセス権限の集中管理
10 違反とセキュリティ活動の報告書
11 障害の処理
12 再認定
13 取引相手の信用
14 取引の認証
15 否認防止
16 信頼できる経路
17 セキュリティ機能の保護
18 暗号鍵の管理
19 不当ソフトウェアの予防，発見，復旧
20 ファイヤウォールアーキテクチャと公共ネットワークへの接続
21 電子的価値の保護

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

組織の上級セキュリティ管理者
情報サービス部門上級管理者およびセキュリティ管理者
情報サービス部門データベース管理者
情報サービス部門セキュリティ管理者
情報サービス部門アプリケーション開発管理者

収集すべき証拠資料:

情報システムセキュリティとアクセスに関する組織的方針と手続
情報サービス部門の，情報システムセキュリティとアクセスに関する方針と手続
以下を含む，適切な方針と手続および法律と規制において主要な情報システムセキュリティの要求
(例：法律，規則，ガイドライン，業界標準)
- ユーザアカウントの管理手続
- ユーザのセキュリティまたは情報保護方針
- 電子商取引に関する標準

(収集すべき証拠資料続き)

- データ分類スキーマ
- アクセスコントロールソフトウェアの一覧
- IT資源を収容する建物／部屋のフロア計画
- IT資源に対する物理的アクセスポイントの一覧またはスキーマ
  (例：モデム，電話回線およびリモート端末機)
- セキュリティソフトウェアの保守管理手続
- 問題の追跡，解消，および段階的修正手続
- セキュリティの違反報告と管理レビューの手続
- データ暗号化機器の一覧と暗号化の標準
- システム資源にアクセスするベンダと顧客のリスト
- データ電送に利用しているサービスプロバイダのリスト
- 継続セキュリティテストに関するネットワーク管理実務
- データ電送のサービスプロバイダとの契約書のコピー
- 承認されたユーザセキュリティと広報文書のコピー
- セキュリティに関する新入従業員訓練項目の内容
- 情報システムセキュリティに関する外部監査人，第三者サービスプロバイダおよび政府機関からの監査報告書

評価視点:

戦略的セキュリティ計画が，集中型の指示を提供するよう整備され，首尾一貫した運用のためユーザのセキュリティ要求に沿って情報システムセキュリティを充分にコントロールする。

集中型のセキュリティ組織が，システム資源に対する適切なアクセスのみを保証する責任を有することが整備されている。

データ分類スキーマが整備運用され，すべてのシステム資源にはセキュリティと内容についてのオーナ責任がある。

ユーザセキュリティプロファイルが，要求に対する最少のアクセスを認めるよう整備され，プロファイルが再確認のため管理者によって定期的にレビューされている。

従業員教育にセキュリティの知識，オーナシップ責任およびウイルス保護要求を含んでいる。

セキュリティの違反報告があり，公式の問題解消手続が整備されている。それらの報告は以下を含んでいる。

- システムへの未承認アクセス (サインオン)
- システム資源への未承認アクセス
- セキュリティ定義，セキュリティルールに対する未承認査閲または変更
- ユーザIDによる資源へのアクセス特権
- 承認された，セキュリティ定義とルールの変更
- 承認された，資源へのアクセス (ユーザまたは資源によって選択される)
- システムセキュリティの状態変更
- オペレーションシステムセキュリティテーブルへのアクセス

(評価視点続き)

暗号モジュールと鍵の保守手続があり，それらが集中的に管理され，すべての外部アクセスと情報伝達行為に利用されている。

集中処理とユーザ処理の両方に対して暗号鍵の管理標準がある。

セキュリティソフトウェア上の変更コントロールが公式で，通常のシステム開発と保守の標準に準拠している。

使用中の認証手続が次の1つ以上の特徴を有している。

- ・認証用データの単一使用 (例えば，パスワードは再使用不可)
- ・多重認証 (例えば，2つ以上の異なる認証方法が使われる)
- ・方針対応認証 (例えば，特定事象に対して，別個の認証手続を特定可能である)
- ・必要時認証 (例えば初期認証の後は，必要に応じて再認証可能である)

同一ユーザの同時セッション数が制限されている。

ログオンの時にハードウェアやソフトウェアの適切な接続を促すためのメッセージが示される。

未承認アクセスの疑いについては，ログオン完了前にスクリーン表示される。

セッション成立後に，当該ユーザのアカウントへの成立アクセスおよび未成立アクセスの履歴が表示される。

パスワードの方針として次のことを含んでいる：

- ・1回目の利用時に初期パスワードの変更を強制する
- ・適切な最小パスワード長
- ・適切で強制的なパスワードの変更頻度
- ・不許可の重要数値リストに対するパスワードのチェック (例えば，辞書チェック)
- ・緊急パスワードの適切な保護

正式な問題解消手順として次のことを含んでいる：

- ・ユーザIDは，ログオンに5回続けて失敗すると使用停止となる。
- ・前回のアクセス時の日付と時刻および不成立なったログオンの回数が，ログオン時に承認されたユーザに表示される。
- ・認証時間は5分に制限されており，それを超えるとセッションは切られる。
- ・ユーザには処理中止が通知されるが，その理由は示されない。

ダイアルインの手順には，ダイアルバックまたはトークンに基づく認証が含まれる。

場所限定方式，は特定の場所における付加的な制限を設けるのに使われる。

ボイスメールサービスやＰＢＸシステムへのアクセスは，コンピュータシステムと同様，同一の物理的および論理的コントロールによって制御される。

機密性の高い職場の方針に次の事項を含める：

- ・機密性の高い仕事を担当する職場の職員は毎年適当な期間その組織から離れなければならない。この間はその職員のユーザIDは使用停止され，その職員の交替要員は，もしセキュリティに関する異常を見つけたら，管理者に報告するよう指示される。
- ・時々，機密事項を扱う職員のローテーションを事前通告なしに行う。

暗号モジュールなどのセキュリティに関連するハードウェアとソフトウェアは，盗聴または漏洩に対して保護され，必要な者のみにアクセスが制限されている。

セキュリティ管理上のセキュリティデータ，機密処理データ，パスワード，暗号鍵へのアクセスは，必要な者のみに制限されている。

信頼性あるパスは，暗号化されない機密情報の伝送に使用される。

(評価視点続き)

いたずらFAXによる攻撃によってサービスが侵害されないよう，次のような保護対策が採られている。
- ・組織外へのFAX番号の開示は必要な者のみに制限する
- ・ビジネスの依頼用のFAX回線は他の用途に使用しない

コンピュータウイルスに関して，予防と検出のためのコントロール対策が管理者によって確立されている。

電子的価値の完全性を確保するため，次のような対策が採られている：
- ・カードリーダ装置は，カード情報の破壊，漏洩，改ざんに対して保護されている
- ・カード情報（PINおよびその他情報）は，インサイダーの漏洩に対して保護されている
- ・カードの偽造が防止されている

セキュリティ上の特徴の保護のため，次の対策が採られている：
- ・認証要求と認証実施のプロセスが特定期間利用されなかった場合は，再手続が要求されること

端末が放置された時に，任意1つのキーでの処理停止などの特別対応処理（one－button lock-up，force button，shut-off sequence）が起動されるようになっている。

► 準拠性テスト:

情報サービス部門が以下に関するセキュリティ標準に従っている。
- ・認証とアクセス
- ・ユーザプロファイルとデータセキュリティ分類の管理
- ・違反とセキュリティ事故の報告，管理者によるレビュー
- ・暗号鍵の管理標準
- ・ウイルスの発見，解消，通知
- ・データ分類とオーナシップ

システムに対するユーザクセスのための要求，確定，および保守の手続があるか。

システム資源に対する外部アクセスのための手続（例：ログオン，ID，パスワード，ダイアルバック）がある。

完全性を保つためのアクセス装置の一覧が維持されている。

オペレーティング・システム・セキュリティ・パラメータがベンダ／ローカルの標準に準拠している。

ネットワークセキュリティ管理実務は周知され，理解され，実施されている。

外部のアクセスプロバイダとの契約書にセキュリティの責任と手続が考慮されている。

システム，ユーザ，および外部のベンダのアクセスに対する実際のログオン手続がある。

諸事故についての適時性，正確性，および管理上の対応に関するセキュリティ報告が実施される。

電送利用のための秘密鍵がある

悪意のソフトウェアから保護するための手順に次のことが含まれている：
- ・組織が入手したすべてのソフトウェアは，インストールして使われる前にウィルスのチェックを実施する
- ・フリーウェアとシェアウェアのダウンロード，利用許諾，使用に関する方針書が存在し，この方針が遵守されている

(準拠性テスト続き)

・非常に重要なアプリケーション用のソフトウェアは，MAC (Message Authentication Code：メッセージ認証コード) またはデジタル署名で保護され，認証を失敗した時はそのソフトウェアの使用を禁止している。
・ユーザはウィルスの発見方法や報告について指示を受けている。例えば，性能の低下やファイルの不可解な増大。
・組織における通常の購買手続をとらないで入手したディスケットの，チェックに関する方針と手続きが存在し，遵守されている。

ファイアウォールは，少なくとも次の特性を持っていること：

・内から外へおよびその逆のすべてのトラヒックは，ファイアウォールを必ず通過する。(これは論理コントロールだけに限定するのではなく，物理的にも実施することである。)
・ローカルのセキュリティ方針の定義に沿って許可されたトラヒックのみが通過可能である。
・ファイアウォール自体がトラヒックの通過に対して免疫性がある。
・ファイアウォールでは，アプリケーション層においてのみトラヒックの交換が行われる。
・ファイアウォールの構成としてアプリケーションとネットワークのレベルにおいてコントロール対策が組み込まれている。
・ファイアウォールの構成としてトランスポテーション層でのプロトコルの不連続性を強制している。
・ファイアウォールは，必要最小限構成の考え方 (minimal art philosophy) で構成されなければならない。
・ファイアウォールの構成として，その構成要素の管理のために厳重な認証が実施されなければならない。
・ファイアウォールの構成として，内部ネットワークの構造を隠蔽する。
・ファイアウォールの構成として，ファイアウォールシステムまであるいはその中を通る，すべての通信の監査証跡を提供でき，怪しい動きを見つけた時にはアラームを出す。
・公衆網から入ってくるサービス要求に対応するための組織のホストは，ファイアウォールの外に置かれる。
・ファイアウォールの構成として，直接攻撃に対して防衛できる。(例えば，能動的なトラヒック監視やパターン認識技術を使って)
・すべての実行可能コードは，内部ネットワークに入れる前に，悪意のあるコード (例えば，ウィルスや悪さをするアプレット) でないかスキャンする。

► 実証性テスト:

類似の組織または適切な世界標準／作業上最適実務に逆らった情報システムセキュリティはない。
コンピュータと伝達資源，その他の物理的および論理的評価の普及を含んだ情報システムセキュリティの詳細なレビューがある。
セキュリティと個々の責任 (例：承認されたセキュリティ文書およびセキュリティに関する新しい従業員の訓練) に対する知識を確かめるための新しい従業員へのインタビューがある。

(実証性テスト続き)

アクセスがビジネス上の必要性（最小限の必要性）に限定されており，正確性を管理することによって規則正しくレビューされていることを確かめるためのユーザへのインタビューがある。

► 実証性テストの結果:

システム資源への不適切なユーザクセス
喪失したアクセスポイントに関するネットワーク図，行方不明の付属品その他に関する一覧の不一致
電送の送信と受信の間のあらゆるポイントにおけるデータのインテグリティとセキュリティに関するオーナシップと責任に対する契約書上の漏れ
規則にあったユーザとして認められない従業員または過去の従業員で未だアクセス権を持っている者
システム資源への非公式または未承認のアクセス要求
セキュリティ違反を警告しないネットワーク監視ソフトウェア
ネットワークソフトウェアの変更管理手続の欠陥
第三者の送受信手続における秘密鍵の未使用
鍵の生成，配付，保管，利用，記録および保護のためのプロトコルの欠陥
ウイルス検査ソフトの陳腐化，または予防，検知，訂正，伝達の侵害防止のための定型手続の不足

DS6 コストの識別と賦課

コントロール目標

1 課金項目
2 原価計算手続
3 ユーザへの請求と課金手続

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報サービス部門管理者またはコスト配分管理者
選定された，コスト負担およびコスト吸収するユーザの管理者

収集すべき証拠資料:

計画と予算作成に関する組織的方針と手続
情報サービス部門のコスト集計，配賦方法論および成果対コストの報告に関する方針と手続
情報サービス部門の次の資料：
- 前期と当期の予算
- IT資源利用の履歴報告
- 履歴報告に用いられた基礎データ
- コストの配分方法論またはアルゴリズム
- 配賦履歴報告

ユーザ管理者の次の資料
- 情報サービス部門コストの前期と当期の予算
- 当期の情報システム開発保守計画
- 配賦コストおよび吸収コストを含むIT資源の経費予算

コントロール評価

評価視点:

情報サービス部門がユーザへの配賦，請求についてその発行，報告をするグループ責任を持っている。
以下の手続が整備されている
- 開発，保守，オペレーション経費の優先順位につきユーザの認識を伴った年間の開発保守計画の作成
- 情報サービス部門の資源が何に費やされているかをユーザが確定する上での高水準の考慮
- 情報サービス部門の年間予算の構成に次が含まれている

(評価視点続き)

・予算作成における組織的要求への準拠
・コストのユーザ部門による配分の首尾一貫性
・配賦コストに何が含まれるかについてのユーザが理解するための，取得原価と新原価
・情報サービス部門よってに配分されるすべての予算コストに対するのユーザの承認
・ユーザに対するコストの実績負担と報告の頻度
・すべてのIT資源の配分コスト履歴（次のようなものだが，それに限定されない）
  ・稼動ハードウェア
  ・周辺装置
  ・通信装置
  ・アプリケーションの開発と支援
  ・管理経常費
  ・外部ベンダのサービスコスト
  ・ヘルプデスク
  ・設備と保守
  ・直接費／間接費
  ・固定費／変動費
  ・埋没原価および裁量原価
・種々のコストの分類を実行するためのユーザに対する定期的報告
・サービスに対する企業期待とユーザの代替資源の比較を可能にするコストの有効性に関する外部の客観的水準についてユーザへの報告
・ビジネス要求の変化を反映させたコスト配分の適時な変更
・受け入れられた請求の公式な承認と受諾
・コスト配賦を減らすまたは配賦コストを基により多くの価値を得るための情報サービス部門の改善の機会の識別

報告は，請求可能な項目が認識しえ，測定しえ，予測しうる保証を提供する。
記録によって，内在するコスト要素または配分のアルゴリズムの変化が捉えられ，強調されていること。

► 準拠性テスト:

コスト配分方法論が存在し，ユーザがその公正さについて同意し，事後の確認のための計算についてコストと報告の両方が作成されている。
コストの低減またはIT資源のパフォーマンス増大のための改善計画がある。
配分と記録によってIT資源の最適で有効的で首尾一貫した利用が促進され，ユーザ部門とその要望の公正な取り扱いが促進されており，且つ請求レートが関連したサービスの提供のコストを反映している。

► 実証性テスト:

同様の組織または適切な世界標準／業界で認められている最適実務に対比して，コスト会計とコストの配賦の基準を決める。
コスト配賦方法論およびユーザからの一連の報告における未処理データからの配賦再計算。
以下のような実績報告へのデータが正しい。

- ･CPU利用率
- ･周辺装置利用率
- ･DASD利用率
- ･記述されたコードのライン数
- ･印刷されたライン／ページ数
- ･実施されたプログラム変更
- ･PC，電話，データファイルの数量
- ･ヘルプデスクの問合わせ
- ･電送の件数と長さ

実績報告への未処理の情報資源データの編集が正しい。
配賦に対するコストの編集と配分のための実際のアルゴリズムがある。
特定のユーザに対する配賦の正確性が頻繁にテストされている。
ユーザに対する配賦は認可されている。
異なるユーザ間で配賦の首尾一貫性チェックがされている。
ユーザの開発計画の進捗は消費されたコストに基づいている。
利用情報およびコスト情報についての分散レビューの報告。
以下に関するユーザ満足度のレビュー。

- ･予算の見込みに対する配賦の合理性
- ･年間の開発計画の進捗対配賦コスト
- ･代替の判断材料（例：ベンチマーク）に対する配賦の合理性
- ･配賦を増加／減少させうる傾向についての意見交換
- ･想定した配賦との変動についての分析

► 実証性テストの結果:

以下について配賦方法論の有効性と適切性を増大させる機会。

- ･より多くのコスト要素の含有
- ･コスト配分の指標または評価の単位の変更
- ･コストアルゴリズム自体の変更
- ･設備とアプリケーション生成記録の間のジョブ会計機能の機械化または統一化

報告書の作成
配分アルゴリズムの首尾一貫性がない。
異なるユーザ間の配分の首尾一貫性がない。
システム資源の改善のための機会がある。

(実証性テストの結果続き)

ユーザのIT資源をユーザのビジネス要求を満たすことに，より適合させるための機会が改善されているか。

サービス提供を受けるユーザにとって実績の改善とコスト削減を別の形で表現する収集，蓄積，配分，報告および意見交換のプロセスにおける有効性が改善されている。

変化と分析の結果を示すコストの傾向は，次期の料金の変更に反映され，コスト体系に影響する。

他の内部や外部のユーザへのサービスを提供する機会を通して，情報サービス部門がコストセンタと言うよりプロフィットセンタとして位置づけられている。

情報サービス部門がプロフィットセンタであるなら，計画と予算に対する利益の貢献は満足するものであり，利益増大のための機会について概要計画がある。

DS7 ユーザの教育と訓練

コントロール目標

1 教育の必要性の識別
2 教育組織
3 セキュリティの原則と意識教育

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

組織の人的資源または教育マネジャ
情報サービス部門の人的資源または教育マネジャ
情報サービス部門の選定されたマネジャと従業員
ユーザ部門の選定されたマネジャと従業員

収集すべき証拠資料:

コントロールとセキュリティ意識教育，啓発的に焦点を合わせた従業員の利益，サービス教育プログラムのユーザ，教育的な資源の施設と専門的な継続教育の要件に関する組織全体の方針と手続
コントロールとセキュリティ意識，技術的セキュリティ，コントロールに関する訓練と教育についての情報サービス部門のプログラム，方針と手続
組織内の予備的および継続的なセキュリティとコントロール意識と教育に関する利用可能な教育プログラム（内部および外部）

コントロール評価

評価視点:

継続的なセキュリティとコントロールの意識に関する方針と手続がある。
情報システムのセキュリティとコントロールの原則に焦点を当てる教育／訓練プログラムがある。
IT資源の使用とカスタディに関するセキュリティ意識とコントロールの責任があることを，新人は意識付けられている。
教育に関連して有効な方針と手続があり，そして，それらがIT資源の技術的構成に関して陳腐化していない。
組織内の教育機会の利用可能性と従業員の出席の頻度
外部の技術的教育機会の利用可能性と従業員の出席の頻度
教育部門は，セキュリティとコントロールに関して，職員の教育ニーズを評価し，組織内または外部の教育機会へ，それらのニーズを反映している。

(評価視点続き)

従業員はすべて，以下のような（これだけに限定されないが），継続してセキュリティとコントロールの意識付け教育に出席するよう求められている。

- 一般的なシステムセキュリティ原則
- 情報サービス部門の倫理行為
- 可用性，機密性，インテグリティ，安全な方法による義務の履行に影響を与える不都合に対し保護するセキュリティ実務
- IT資源の保管と使用に関連する責任
- オフサイトでの情報および情報システムのセキュリティ

セキュリティ意識教育には会話による機密情報の暴露を防止する方針も含まれる。（例えば，会話に参加した人々に情報の位置づけをアナウンスするなど）

► 準拠性テスト:

新人は，IT資源の所有と使用に関するセキュリティとコントロールと信用上の責任を知っており理解している。

すべてのIT資源の機密性，インテグリティ，可用性，信頼性およびセキュリティに関する従業員の責任は，継続的に伝達されている。

情報サービス部門グループは，専門的な認定について，公式にIT教育，セキュリティとコントロール意識，継続して教育プログラムを維持するのに責任がある。

従業員の教育ニーズの継続的評価が行われる。

セキュリティとコントロールに関連する教育プログラムへの開発または参画が，教育要件の一部である。

新人および長期雇用者のセキュリティ意識について，実際の教育プログラムがある。

機密保持および利害関係記述書が従業員すべてによって署名される。

従業員についての機密保護および利害関係記述書についての抜けがない。

従業員についての教育ニーズの評価に抜けがない。

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:

セキュリティ，機密性，信頼性，可用性，インテグリティのコントロールについて，教育マニュアルが適切かつ十分であることのレビュー。

教育ニーズの識別，それらのニーズの履行程度を確かめるための，情報サービス部門スタッフへのインタビュー。

► 実証性テストの結果:

教育ニーズに対応して，提供されたカリキュラムの不整合

IT資源の利用に関するセキュリティと内部コントロールの問題についてのユーザの意識の欠如

DS8 ITのカスタマへの支援と助言

1 ヘルプデスク
2 カスタマ照会の登録
3 カスタマ照会の上申
4 照会回答済みのモニタリング
5 傾向の分析と報告

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報サービス部門のヘルプデスク支援マネジャ
情報サービスの選定されたユーザ

収集すべき証拠資料:

情報サービス部門のユーザ支援に関する組織全体の方針と手続
ヘルプデスク活動に関する情報サービス部門の規程，使命，組織図，方針と手続
ヘルプデスクのユーザ照会，照会の解決，実施統計に関する報告書
ヘルプデスク活動についての実施標準
情報サービス部門と様々なユーザ間のサービスレベルアグリーメント
ヘルプデスクスタッフの経験および専門性の概要を証明する人事ファイル

コントロール評価

評価視点:

ヘルプデスク機能の性質（つまり，支援の要望が処理され，支援が行われる）が有効である。
実際の機能，部門または部門がヘルプデスク機能を実施し，個々人または職位にヘルプデスクの責任がある。
ヘルプデスク活動についての文書化のレベルが適切で最新である。
ロギングまたはログのサービスと使用の要求の登録について実際のプロセスがある。
照会の上申と解決するための管理者の関与のプロセスが十分である。
受領した照会を処理する時間が適切である。
ヘルプデスク活動の傾向の追跡と報告の手続がある。
実施向上の活動が公式に明らかにされ，実行される。
サービスレベルアグリーメントと実施標準が満足されている。
ユーザ満足度のレベルが定期的に判定され，報告されている。

► 準拠性テスト:

方針と手続がヘルプデスク活動について，最新で正確である。
サービスレベルのコミットメントが遵守され，差異が説明されている。
照会の措置が適時に行われている。
傾向分析と報告書によって，以下を報告する保証を与えている。
- ・作成され，傾向はサービス向上について示される。
- ・特定の問題，傾向分析，レスポンスタイムを含む。
- ・問題を解決するために，権限を持った責任ある個人に伝えられる。

ヘルプデスクの依頼，正確さの確認，適時性を対応の十分なサンプル
ユーザ満足度レベルの質問事項が存在し，実施されている。

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:

以下の満足度を確認するために，選定されたユーザにインタビューする。
- ・ヘルプデスク活動
- ・活動報告
- ・サービスレベルコミットメントの会議

義務の遂行に関して，経るスタッフの能力と権限をレビュー
対応の適切さについて，上申された照会を選んでレビュー
傾向と可能な実行強化機会の報告をレビュー

► 実証性テストの結果:

ユーザ組織同様，情報サービス部門内で，他の部門に関して，ヘルプデスク活動の不適切な相互作用
　問題報告照会の受領，登録，ロギング，追跡，上申，解決に関連する不十分な手続と活動
管理者の関与の欠如または有効な是正活動に関する欠陥のある上申プロセス
問題報告書または問題報告書プロセスのユーザの不満足の不適切な適時性

DS9 構成管理

コントロール目標
1 構成の記録 2 構成のベースライン 3 状況の説明 4 構成のコントロール 5 違法ソフトウェア 6 ソフトウェアの保管

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報サービス部門の運用管理者
情報サービス部門のシステムサポート管理者
情報サービス部門のアプリケーション開発管理者
施設管理者
ソフトウェアベンダサポート担当者
コンピュータ関連資産管理担当者
品質保証管理者

収集すべき証拠資料:

オンサイトおよびオフサイトの構成一覧:ハードウェア, オペレーティングシステム・ソフトウェア, アプリケーションソフトウェア, 施設, そしてデータファイル
購入, レンタル, リースの対象であるコンピュータ関連設備とソフトウェアの取得, 有高管理, 処分に関する組 織上の方針と手続
未承認のソフトウェアや設備の使用に関する組織上の方針
構成資源の取得, 処分, メンテナンスに特に関連する情報サービス部門の方針と手続
情報サービス部門の品質保証に関する方針と手続, および, 新規のそして修正されたソフトウェアの開発から本番への状況やファイルへ移行する独立した移動と記録の変更統制機能
情報に基づく構成
システム資源に関する固定資産とリースの会計記録
システム構成への追加, 削除, 変更に関する報告
テスト, 開発, 本番における種々のライブラリ内容のリスト
供給者の手元にある資料を含む設備, ファイル, マニュアル, 書式用紙のオフサイト保管内容の一覧

コントロール評価

► 評価視点:

構成ベースラインを作成し，統制するプロセス（変化が厳密な構成コントロールを受けることなしでは生じない構成項目の設計と開発における締め切りポイント）が適切であること。
構成ベースラインを維持する機能が存在すること。
入力，出力，そして他のプロセスとの統合を含む，購入，リースの資産についての会計状況報告を統制するプロセスが存在する。
構成コントロール手続は以下を含んでいる。

- ・構成ベースラインインテグリティ
- ・変更管理システム上のプログラムされたアクセス権限コントロール
- ・構成項目の復旧とあらゆる時の変更要求
- ・構成の完了と構成記録手続の適切性を評価するレポート
- ・構成を記録する機能の定期的な評価
- ・構成コントロールをレビューすることに責任がある個人に必要な知識，技能，才能がある
- ・ソフトウェアベースラインへのアクセスをレビューするための手続が存在する
- ・調整の行動のためにレビューの結果が管理者に与えられること

有高管理と会計記録による構成の定期的なレビューが，一定の基準で行なわれる。
変更を追跡するために構成ベースラインは十分に履歴をもつ。
以下のソフトウェア変更統制手続が存在する。

- ・認可を受けたアプリケーションプログラムライブラリを作成し，維持する
- ・認可を受けたアプリケーションプログラムライブラリが適切に統制されることを保証する
- ・ソフトウェア目録の信頼性とインテグリティを保証する
- ・使用される承認されたソフトウェアの目録の信頼性とインテグリティを保証し，未承認ソフトウェアをチェックする
- ・具体的なスタッフメンバに未承認ソフトウェアの統制に対する責任を割り当てる
- ・未承認ソフトウェアの使用を記録し，調整行動を管理者へ報告する
- ・管理者が違反に対する調整行動をとったかどうか評価する

開発中のアプリケーションをテスト環境へ移行し，そして最終的に本番状況に移行するプロセスは，構成レポートと互いに作用し合う
ソフトウェア保管プロセスは以下を含む。

- ・システム開発ライフサイクルの適切な段階で，すべての有効なソフトウェアのために安全なファイル保管領域（ライブラリ）を定める
- ・ソフトウェア保管ライブラリはお互いに，そして開発，テスト，本番ファイル保管領域から分けられることを要求する
- ・ソースモジュールの一時的なロケーションを本番サイクル期間に移行することを許すソースライブラリ内の存在を要求する
- ・すべてのライブラリの各メンバに所有者が割り当てられることを要求する
- ・論理的，物理的アクセス管理を定める
- ・ソフトウェア報告責任を確立する
- ・監査証跡を確立する
- ・この手続に準拠しないすべての場合を見つけ，文書化し，管理者に報告する

(評価視点続き)

・管理者が調整行動をとったかどうか評価する

変更への構成ベースラインを更新することに関してアプリケーション開発，品質保証，オペレーションの間で調整が行なわれる。

準拠性テスト:

すべての構成項目がベースラインのコントロール下にある。
構成報告に関する方針と手続が最新であり，正確である。
構成の保守と報告に関する実施標準が守られている。
設備と資産の会計記録の物理的な一覧に対する構成ベースラインの比較がある。
テストから本番への独立した移行と変更の記録がある。
以下のベースライン出力の選択に対して，

- ・正確で，適切な，承認されている構成項目のベースラインが保たれている
- ・構成記録は，変更履歴を含むすべての構成項目に対して実際の状態を反映している
- ・構成記録の一貫性が管理者によって定期的にレビュー，評価され，調整行動がとられている
- ・ファイルライブラリが適切に十分に定められ，システム開発ライフサイクルの適切なフェーズにある
- ・未承認ソフトウェアを保持し，違反のすべてのパーソナルコンピュータが報告され，管理者が調整行動をとっている
- ・製品，バージョン，すべてのベンダ提供資産への修正に関する構成記録が正確である
- ・構成への変更履歴が正確である
- ・以下にあげるものを含み，未承認ソフトウェアがコンピュータ上にないことを保証するためのメカニズム
  - ・方針と記述
  - ・潜在的な債務（法的債務と製品に起因する債務）の研修と周知
  - ・コンピュータを使っているすべてスタッフによる遵守すべき署名書式
  - ・コンピュータソフトウェアの集中コントロール
  - ・コンピュータソフトウェアの稼動中のレビュー
  - ・レビューの結果報告
  - ・レビュー結果に基づく管理者による調整行動
- ・アプリケーションプログラムとソースコードの保管が開発サイクルの中で決められ，構成記録への影響が確かめられている。
- ・構成に関するオフサイトとベンダ記録の十分性とインテグリティ，構成記録の正確性が予想され，熟慮されている。
- ・以下に対して構成ベースラインの手続が定義される
  - ・ベースラインを作ったできごとの記録，ベースラインの確立，そしてベースラインで統制される構成項目
  - ・以前に承認されている構成ベースラインへの変更を承認するために要求される権限を含んでいるベースラインの変更

(準拠性テスト続き)

・ベースラインへの変更とベースラインで統制される構成項目の記録
・すべての構成項目がベースライン製品で記録されることを保証すること
・以下のものに対して，会計報告の状況がある
・収集され，保管され，処理され，報告される情報の種類（これはベースラインの状態，ベースラインレビューの発見，変更要求と状態，（もし適用できるならば）構成コントロールボードレビューと承認／非承認，実際に行なわれた変更，トラブル報告と状態，構成の改訂履歴を含むべきである）
・不完全な状態報告で変更要求課題がどのように解決されたか
・作成された会計報告の状況のタイプと頻度
・この状態データへのアクセス方法がどのように統制されるか

► 実証性テスト:

構成記録，記録への変更，有高目録と会計報告とベンダ記録との一致に対する管理者レビューの頻度と適時性の詳細なレビュー

重複可能な種々のライブラリのコンピュータ化されたソフトウェア分析，除去されたオブジェクトコードの確認，不要なデータやプログラムの削除，そして構成記録への反映

► 実証性テストの結果:

以下に関する管理者とスタッフの組織的な方針の認識と理解の弱点
・それらの記録への構成記録と変更
・システム開発ライフサイクルでの構成コントロールの配置
・構成，会計記録，ベンダ記録の統合
・パソコン上の未承認ソフトウェアの非使用

ベースライン構成作成と保守機能の有効性や効率性における可能な改良の不適当さ

構成記録に反映されているベンダ変更の欠陥，記録セキュリティ，適切に反映されているベンダによる記録の変更

DS10 問題と障害管理

コントロール目標

1 問題管理システム
2 問題の上申
3 問題の追跡と監査証跡

高レベルかつ詳細なコントロール目標の監査手続

理解

► 面接対象者:

情報サービス部門の運用支援スタッフ
情報サービス部門のヘルプデスク支援スタッフ
情報サービス部門のシステム支援スタッフ
情報サービス部門のアプリケーション支援スタッフ
IT 資源の選定されたユーザ

► 収集すべき証拠資料:

問題管理機能を実現する問題管理施設と位置のまとめ
認識，ロギング，解決，上申，追跡，報告プロセスを含んでいる問題管理に関する情報サービス部門の方針と手続
発生日，(適応できるならば) 上申日，解決日，解決のための時間枠を含む対応期間に報告された問題の一覧
優先的解決のため上級管理者の応対のため直ちに上申した，あるいは重大な問題として報告すべき重大なアプリケーションの一覧
あらゆる問題管理アプリケーションの識別。確認のための特別な方法により，すべての問題が把握され，解決され，要求に応じて報告される

コントロール評価

► 評価視点:

標準運用の一部ではないすべての運用結果が記録され，分析され，適時に解決されることを保証する問題管理プロセスがあり，障害報告は重要な問題として生成される。
以下のような問題解決手続があること。

- 問題管理システムを定義し，導入する
- 標準にないあらゆる事象を記録し，分析し，適時に解決する
- 重要な事象に対して障害報告を確立し，ユーザに報告すること
- 問題の種類を明らかにすることとリスクに対応した解決策を与える優先付け方法論

(評価視点続き)

・問題管理情報の論理的，物理的コントロールを定義する

以下のような問題解決手続がある。

・必要な者のみに提供されるという原則に基づきアウトプットを分類する
・資源を最大にし，所要期間を縮めるために問題の傾向を追跡する
・報告するための正確な，最新の，矛盾のない，利用できるデータ入力を収集する
・上申と周知に対する管理者の適切なレベルを通知すること
・増加した有効性と効率性に対する問題管理プロセスを管理者が定期的に評価するかどうかを確定すること
・システム問題に対する監査証跡の十分性
・変更，可用性，構成管理システム，個人のインテグレーション

準拠性評価

► 準拠性テスト:

プロセス出力の選択されたサンプルが以下に関する公式の手続に従っている。

・重大ではない問題
・上申を要求する高いプライオリティ／重大な問題
・報告の要求，内容，正確さ，配付，とられた行動
・問題管理プロセスと結果のユーザ満足

インタビューによって，問題管理プロセスの周知と理解

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:

報告された問題から選択したものについて，問題管理手続が以下を含むすべての標準でない行動に対して遵守されているか確かめるためにテストする。

・プロセスによるすべての標準でない事象を記録する
・それぞれすべての事象を追跡し，解決する
・事象の優先順位に基づくレスポンスの適切なレベル
・重大な事象に対する問題の上申
・情報サービス部門とユーザグループ内の適切な報告
・改善に対するプロセス有効性と効率性の定期的なレビュー
・改善プログラムの予想と成功のパフォーマンス

► 実証性テストの結果:

問題管理プロセスによって正式にはコントロールされない問題の存在
問題管理プロセスによって認識されるが解決されない問題の存在

(実証性テストの結果続き)

問題解決に関して事象の実際のプロセスと正式なプロセスとの間の相違
可能な改善の機会に対して，問題管理プロセスのユーザ欠点，問題についての意思疎通と解決

DS11 データ管理

コントロール目標

1 データ作成の手続
2 原始ドキュメントの承認手続
3 原始ドキュメントのデータ収集
4 原始ドキュメントエラーの取扱
5 原始ドキュメントの保存
6 データ入力承認手続
7 正確性，完全性，および承認チェック
8 データ入力エラーの処理
9 データ処理のインテグリティ
10 データ処理の妥当性と誤謬摘示
11 データ処理エラーの取扱
12 出力の取扱と保存
13 出力の配付
14 出力の合計突合と照合調整
15 出力のレビューとエラーの取扱
16 出力報告書のセキュリティ条項
17 伝送と輸送中における機密情報の保護
18 廃棄機密情報の保護
19 保管管理
20 保存期間と保管条件
21 媒体ライブラリ管理システム
22 媒体ライブラリ管理の責任
23 バックアップと復旧
24 バックアップ・ジョブ
25 バックアップ保管
26 保管
27 機密メッセージの保護
28 認証とインテグリティ
29 電子取引のインテグリティ
30 記憶データの継続的なインテグリティ

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

情報サービス部門の運用管理者
情報サービス部門のデータベース管理者
情報サービス部門のアプリケーション開発管理者
情報サービス部門の人的資源／研修管理者
情報サービス部門のシステム支援管理者
バックアップサイトのセキュリティと一般管理の管理者
重要な任務を行うアプリケーションに対する種々のユーザ管理者

► 収集すべき証拠資料:

以下を含むデータの特徴と管理に関する組織的な方針と手続

- ･情報サービス部門内のデータフローおよびユーザへ／からのデータフロー
- ･データが発生し，バッチ処理され，編集され，入力され，処理され，出力され，レビューされ，訂正され，再実行され，ユーザに配付される組織内のポイント
- ･原始ドキュメント承認プロセス
- ･データ収集，トラッキング，送信プロセス
- ･入力に対する完全な原始ドキュメントについて正確さ，会計処理，伝達を保証するための手続
- ･データ発生の間にエラーを認識し，訂正するために使われる手続
- ･インターネットその他の公衆網を介して伝送される機密メッセージの完全性，信頼性，否認不可を保証する手続
- ･原始ドキュメント（記録すること，画像化することなど）を保持するために組織によって使われる方法，どの文書が保管されるべきか，法規の要請など。
- ･情報サービス部門のデータを提供し，利用するインタフェース･システム
- ･データ管理タスクを行なうベンダ契約
- ･活動と一覧をモニターするために使われる管理報告

以下にあげるものに関するすべての主なアプリケーションとユーザドキュメンテーションのリスト

- ･入力の正確さ，完全，承認チェックを行なっているモジュール
- ･各々のアプリケーションにデータエントリーを行なっている機能
- ･データエントリーエラー訂正処理を行なっている機能
- ･エラーを防ぎ（手動やプログラムによる手段），発見し，訂正するために使われる方法
- ･実行されたデータの処理のインテグリティを管理する
- ･できるだけ発生源へ近づいたデータ処理編集誤謬摘示と認証
- ･アプリケーションから生成された出力の取り扱いと保管
- ･出力，出力の配付，出力を使っているインタフェース･システム
- ･合計と相違の調整を管理するために出力の残高調整手続
- ･出力レポートと情報の正確さをレビューする
- ･分散処理出力レポートを保証すること
- ･伝送されたデータとアプリケーション間を保証すること
- ･取り扱いに慎重を要する入力，プロセス，出力のドキュメンテーションを処分すること
- ･準備，入力，処理，出力のサードベンダ管理手続

組織のあらゆるセントラルデータベースリポジトリに関する方針と手続は以下にあげるものを含んでいる。

- ･データベースの構成とデータディクショナリ
- ･データベースのメンテナンスとセキュリティの手続
- ･データベースの所有権の決定とメンテナンス
- ･データベース設計と内容上の変更コントロール手続
- ･データベースの活動を明らかにしている管理報告と監査証跡

メディアライブラリやデータのオフサイト保管に関する方針と手続が以下にあげるものを含んでいる。

- ･メディアライブラリとライブラリ管理システムを管理する
- ･すべてのメディアについて外部の認証を要求する

(収集すべき証拠資料続き)

・活動をコントロールするためにすべての内容とプロセスについて最新の一覧を要求する
・データ資源を保護するための管理手続
・実際とデータ記録の間の調整手続
・データメディアのデータを再生，交替
・過去のテスト・データ一覧と行なわれた復旧テスト
・継続性計画におけるメディアとオフサイトの運用者の役割

► 評価視点:

データ準備に対して

・データ準備の手続は完全さ，正確さ，正当性を保証する
・すべての原始ドキュメントに対して承認手続がある
・発生，承認，原始ドキュメントからデータへの変換の間について職務の分離がある
・原始ドキュメントの発生源を通して，承認されたデータが完全で，正確で，妥当である
・データが適時に伝達される
・正確な完了と承認のために原始ドキュメントの定期的なレビューがある
・誤った原始ドキュメントの適切な取り扱い
・妥協からの保護のために取り扱いに慎重を要する情報上の十分なコントロールが原始ドキュメント上にある
・手続は原始ドキュメントの完全さと正確さ，原始ドキュメントのための正確な会計，そして適時なコンバージョンを保証する
・損失の場合の再現，レビューと監査での利用，訴訟や規則の要請のために，原始ドキュメントの保管は十分に長くとられていること

データ入力に対して

・エントリー前の承認のための適切な原始ドキュメントの配付経路付け
・上申，査閲，承認，データエントリー機能間の職務の正確な分離
・唯一無二のターミナルあるいはステーションコード，保証されたオペレータ識別
・ステーションコードとオペレータIDの使用，維持，管理
・入力のソースを識別する監査証跡
・できるだけ発生源へ近づいた入力データのルーチン的な確認あるいは編集チェック
・誤って入力されたデータの適切な取り扱い
・データ上で正確な認証を施行することに対するはっきりと割り当てられる責任

データ処理に対して:

エラーの防止，発見，訂正のルーチンを含むプログラム:

・プログラムはエラー（すなわち，確証と編集）に対する入力のテストを行なわなければならない
・プログラムは，同じマスタリストに対するすべての取引を承認しなければならない
・プログラムはエラー条件の無効を拒絶しなければならない

(評価視点続き)

エラーの取り扱い手続は以下を含むこと:
- ・エラーの訂正と再実行は承認されなければならない
- ・サスペンスファイルに対する個人の責任が定義されている
- ・解決されていないエラーに対してサスペンスファイルがレポートを生成する
- ・サスペンスファイルの優先付け計画は世代とタイプに基づいて利用できる

監査証跡のための実行されたプログラムと処理された／拒絶された取引のログが存在する
すべての処理されたデータに対して件数と合計の残高調整と一緒に，入力処理をモニターし，標準でない事象を調査するためのコントロールグループ
たとえ1つのフィールドにはエラーがあるとしても，すべてのフィールドが適切に編集される
確証で使われるテーブルは，時々レビューされる
再処理するために混乱を起こさせない解決を含んでいるエラーの中でデータを訂正し，再実行することの文書化された手続が存在する
再実行された取引は，元々の処理と同じように正確に処理されること
エラー訂正に対する責任は，オリジナルの実行機能に存在する
人工知能システムは極めて重大な決定は人間のオペレータが承認しなければならないように，双方向のコントロールの枠組みの中で位置付けれれている

出力，インタフェース，配付に対して:

出力へのアクセスは，認可された人に物理的に論理的に制限される
出力の必要性について実施中のレビューがある
出力は関連するコントロール合計といつも残高調整される
監査証跡が取引処理のトレーシングと分けられたデータの一致を容易にするために存在する
出力レポートの正確さがレビューされ，出力に含まれるエラーを認識した人員によって管理される
出力，インタフェース，配付間のセキュリティ問題の明確な定義が存在する
あらゆるフェーズ間のセキュリティ違反のコミュニケーションが管理者に伝達され，実行され，適切に新しい手続に反映される
出力に対するプロセスと責任の配置がはっきりと定義されている
処理後に必要でなくなった使用済み資料の廃棄が証明される
直近の事態に備えて，すべての入力と出力のメディアがオフサイトロケーションに蓄積される
削除とマークされた情報は，二度と取り出されないような方法で変換される

メディアライブラリに対して:

メディアライブラリの内容が，システム的に一覧に記入される
一覧で明らかにされた不一致が適時に改善される
ライブラリに格納された磁気メディアのインテグリティを維持するための手段がとられる
メディアライブラリの内容を保護するために管理手続が存在する
メディアライブラリ管理に対する責任は，情報サービス部門スタッフの具体的なメンバに割り当てられる
メディアのバックアップと復旧の計画が存在する
メディアバックアップは，定義されたバックアップ計画と一致するように行なわれ，バックアップの有用性が定期的に確かめられる

(評価視点続き)

メディアバックアップは安全に格納され，保管場所は物理的なアクセスセキュリティやデータファイルのセキュリティやその他の項目に関して定期的にレビューされる
文書，データ，プログラム，レポートおよびメッセージ（入力，出力）は，それらの暗号化や証明に使われるデータ（鍵や証明書）と同じように保存期間や保管条件が定義される
紙のドキュメントの保管に加えて，電話での会話も記録し保存すること－但し，ローカルのプライバシー法に抵触しない場合－電話で伝統的に行われているビジネス活動の一部である取り引きやその他の会話について，上記措置をとれる
法的要件やビジネス要件に沿った情報（データとプログラム）の公的保管場所に関する適切な手続があり，報告責任や複製が満足できるようになっている

情報の証明とインテグリティに関して：
データファイルのインテグリティが定期的にチェックされる
電話またはボイスメールを介して組織の外部から来る問い合わせは，コールバックまたはその他の認証方法で身元確認をする
ＦＡＸまたはイメージシステムを介して受け取る問い合わせの発信元と内容の認証の独立した確認のために予め用意した方法が使われる
電子署名または電子証明が，入手した電子ドキュメントのインテグリティの確認や内容証明のために使われる

► 準拠性テスト:

データ準備：
選び出されたサンプルの原始ドキュメントに対して，承認，査閲，正確性，完全性，データ入力による受領に関する記述された手続に対する一貫性が明白であり，データ入力がタ適時である
原始ドキュメント，入力，データ変換スタッフはデータ準備コントロール要求を知り，理解する

データ入力：
正確性，完全性，許可チェックを保証するためのテスト･データ（正，誤の取引タイプ）が行なわれる
選び出された取引に対して，入力前後にマスタファイルが比較される
エラーを扱う保留，解決，適切なレビューインテグリティが存在すること
エラーを扱う手続と行動は，確立された方針とコントロールに応じている

データ処理：
ランツーランコントロールトータルとマスタファイル更新コントロールが有効に使用される
できるだけ起点ポイントに近づいたデータ処理の確証，認証，編集を保証するためのテスト･データ（正，誤の取引タイプ）の実行が行なわれる
確立された手続とコントロールに従って，エラー取り扱いプロセスが行なわれる
エラーの取り扱いの保留，解決，適切なインテグリティレビューが存在し，適切に機能している

(準拠性テスト続き)

エラーの取り扱い手続と行動は確立された手続とコントロールに応じている

データ出力，インタフェース，配付：

出力は関連するコントロール合計にいつも残高調整されている
監査証跡が取引処理の追跡と分散されたデータの調整を容易にするために提供される
出力レポートは，供給者と関連ユーザによって正確さをレビューされる
エラーの取り扱いの保留，解決，適切なインテグリティレビューが存在し，適切に機能している
エラーの取り扱い手続と行動は確立された方針とコントロールに応じている
出力レポートは，すでに確立された手続とコントロールに応じてユーザに配付されたのと同じように用意されている配付を守られる
権限がないアクセスと修正に対して伝達とトランスポートの間に，取り扱いに慎重を要する情報に十分な保護が存在する
処分された機密情報についての手続と行動が，確立された方針とコントロールに応じている

メディアライブラリ：

メディアライブラリの内容がシステム的に一覧に記入され，明らかにされた不一致が適時に改善され，ライブラリに格納されたメディアのインテグリティを維持するために手段がとられる
メディアライブラリの内容を保護するために設計された管理手続が存在し，適切に機能している
メディアライブラリ管理に対する責任が適切に割り当てられる
メディアライブラリが，準備，入力，処理，出力の機能から独立している
メディアのバックアップと復旧の計画が適切である
メディアバックアップが，定義されたバックアップ計画に従って適切に行なわれている
メディアの保管場所が物理的に安全であり，管理目録は最新である
データ保管は検索要求とコスト有効性を考慮に入れる
文書，データ，プログラム，レポートに対して，保存期間と保管条件が適切である

情報の内容証明とインテグリティについて：

インターネットやその他の公衆網を介して伝送される機密メッセージのインテグリティ，機密性，否認不可を適切な手続で保証する
メッセージのアドレスを間違えるリスク（手紙，ＦＡＸ，電子メールにおいて）が適切な手続により軽減される
ＦＡＸや自動電話メッセージ応答のような特別な処理やプロセスに通常適用されるコントロールが，そのような処理やプロセスを行うコンピュータシステム（例えば，パーソナルコンピュータ上のＦＡＸ処理ソフト）にも適用される

実証性テスト:

類似した組織に対するデータ管理をベンチマークすること，あるいは適切な国際標準／承認された業界の最適実務

選択された取引に対して，以下にあげるものの間に正確に処理することを確認する

- ･データ準備
- ･入力処理
- ･データ処理
- ･出力，配付，統合
- ･すべての処理フェーズにおけるエラーの取り扱い
- ･すべての処理フェーズにおけるエラーの取り扱いを通したデータのインテグリティ
- ･保管と破棄

以下に対して明確にテストする

- ･各処理フェーズ間の完全性，正確性，妥当性
- ･適切な承認と許可
- ･処理内に，コントロールグループマニュアル／手続部門を通して予防，発見，訂正コントロールがある
- ･最近要求されたレビューに対して，原始ドキュメントの保管が保管要件と一致する
- ･原始ドキュメントと取引メディアの選択を検索し，存在と正確さを確かめる
- ･監査証跡の可用性を分析する：ソース／オペレータを識別が存在する，システムのあらゆるインタフェースが取引において等しいレベルのコントロールを持つ
- ･入力時，編集する項目や処理プログラムは以下を含む，ただしこれに限らない：
  - ･必要なフィールド中のブランク
  - ･取引コードの確認
  - ･負の金額
  - ･すべての他の適切な状態
- ･処理の内部確証テストの十分性
- ･不完全な取引のあるサスペンスファイルは，次のコントロールを含む：
  - ･エラーをしているオペレータの即時の識別とエラーの通告
  - ･すべてのエラー取引は，これらのサスペンスファイルへ移動される
  - ･取引が解決され，移動されるまで，記録が保持される
  - ･取引はエラーコード，入力の日時，オペレータ／マシンを示す
  - ･サスペンスファイルがマネジメントレビュー，傾向分析，改善的なトレーニングのためにフォローアップ報告を作成すること
- ･発生，入力，処理，検証，配付の機能の分離

アウトプット取引の選択に対して：

- ･完全性と正確性のために処理されたリストの取引のサンプルをレビューする
- ･正確性と完全性のために出力レポートのサンプルをレビューする
- ･手続への適切性と準拠性のために出力保管スケジュールをレビューする

(実証性テスト続き)

- 正確に配付された出力のサンプルについて実際の配付を確かめる
- 出力の1つと他システムの取引ログの入力を確かめることによって統合化された処理を確かめる
- すべての入力，処理している出力，他システムで使用する取引に対して手続きのバランスをレビューする
- 承認された要員だけが要注意のレポートにアクセスすることを確かめる
- 保管方針と手続に従い，すべてのデータメディアに対して破棄かオフサイトの保管場所への移動を確かめる
- 保管手続に対して実際の保管期間を確かめる
- 要注意の出力について実際の配付あるいは伝達の証拠，そして処理，配付，セキュリティ手続への準拠性
- 継続性計画の要件と同様に正常な処理に関連するバックアップ生成とインテグリティを確かめる

メディアライブラリに対して：

- 要注意のユーティリティーへのユーザクセスをレビューし，そのアクセスが適切であることを決定する
- 破壊されたメディアのサンプルを選択し，全体のプロセスを観察する；承認されている手続への準拠性を実証する
- オフサイトの保管場所にあるデータや伝送中のデータに対するコントロールの適切さを判定している
- ほとんど最近のメディアライブラリ目録の結果を得る；正確さを確かめる
- 保管しているプロセッサ記録が必要なメディアにアクセスするのに十分であることを確かめる
- 内部と外見を分類しているルールのバイパスを制限することに対するコントロールのレビュー
- 選択されたメディアのレビューを通して，外部，内部コントロールの準拠性をテストする
- 災害の場合に十分なデータを保証するために，バックアップ生成手続をレビューする
- 予定された要件についてのメディアライブラリの検査を確かめる

► 実証性テストの結果:

オペレータが本番ファイルに直接アクセスした時，ファイルの「前」と「後」のイメージが生成されないで，メンテナンスされる

機密性のある入出力フォーム（すなわちチェックストック，ストック証明書）が保護されていない

処理のすべてのフェーズに対するバッチとコントロールトータルのログが保たれていない

出力レポートがユーザにとって有用でない：データが適切でなく有用でもない，レポートが不要のものである，その配付先が不適切である，そのフォーマットと頻度が適切でない，レポートへのオンラインアクセスがコントロールされていない

伝送されたデータに対して，以下のことを含んだ付加的なコントロールがない

- 送受信アクセスの制限
- 送り手と受け手に対する適切な認証と識別
- 伝送のための安全な方法
- 伝送されるデータの暗号化と適切な復号化アルゴリズム

(実証性テストの結果続き)

・完全さに対する伝送のインテグリティテスト
・再伝送の手順

破棄サービスのようなコントロールを逃しているベンダとの契約
火，水，電気，そして未承認アクセスのような環境の危険に関するオフサイトの欠陥

DS12 ファシリティ管理

コントロール目標

1 物理的セキュリティ
2 目立たないITサイト
3 訪問者への付添
4 要員の健康と安全
5 環境要因に対する保護
6 無停電電源装置

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

施設管理者
セキュリティ担当役員
リスク管理者
情報サービス部門運用管理者
情報サービス部門セキュリティ管理者

収集すべき証拠資料:

施設管理，レイアウト，セキュリティ，安全，固定資産目録，資本取得／リースに関する組織の方針と手続
施設レイアウト，物理的，論理的セキュリティ，安全，アクセス，保守，信号系，訪問者，健康，安全，環境要件，入出口機能，セキュリティ報告，セキュリティと保守の契約， 設備の目録，監視手続，規則要件に関する情報サービス部門の方針と手続
施設と施設のフロアレイアウトにアクセスする個人のリスト
産業標準を含んでいる，情報システム資源（設備と施設）の実行見込みに関連がある実行，能力サービスレベル協定のリスト
継続性計画文書のコピー

コントロール評価

評価視点:

施設ロケーションは外部対し明確に表示せず，最少限のアクセスを許すエリアあるいは組織とし，アクセスは最少の人員に限られている
論理的，物理的アクセス手続は十分であり，従業員，ベンダ，設備，施設保守スタッフに対してセキュリティアクセスプロフィールを含んでいる
「鍵」と「カードリーダ」の管理手続と実施は十分であり，稼動中のアップデートと必要な最小アクセス基準によるレビューを含んでいる

(評価視点続き)

すべてのエリア，特に機密エリアへの入退室のアクセスと認証の方針，付き添い，登録，一時的に必要なパス，および監視カメラの設置が適切である
マネジメントレビューを含んで，定期的，稼動中のアクセスプロフィールのレビューが行なわれている
セキュリティ違反が発生した時，取り消し，応答，上申プロセスが実行される
セキュリティおよびアクセスコントロール対策に移動型またはオフサイトで使用できる情報装置も含めている
信号系は，取り扱いに慎重を要しない場所に設置し，保険，ローカルの建築法，規則要件に準拠している
訪問者登録，パス割り当て，付き添い，訪問者に対する責任者，入退を保証する記録帳，セキュリティ手続を理解している受付係のレビューがある
火災，天候，電気警告とアラームの手続のレビュー，環境上の非常時の種々なレベルに対して予想される応答シナリオがある
空気調和，換気，湿度コントロール手続，そして種々な損失あるいは予期できない危機に対して予想される応答シナリオについてレビューがある
以下にあげるものを含み，セキュリティ違反アラームプロセスのレビュー結果がある：
- ・アラームの優先度の定義（すなわち，構内で武装した爆弾兵に通ずる風の通気孔のドア）
- ・各々の優先アラームへの応答シナリオ
- ・組織内の人員対ローカルあるいはベンダセキュリティ人員の責任
- ・ローカルの監督官庁との相互作用
- ・最近のアラーム訓練のレビュー

以下にあげるものを含む情報サービス部門内の物理的アクセスに対して組織は責任がある
- ・開発，保守，セキュリティ方針と手続の稼動中のレビュー
- ・セキュリティ指向のベンダとの関係を確立する
- ・セキュリティと関連がある技術問題に関する施設管理者間の連絡
- ・組織に対するセキュリティ認識とトレーニングのコーディネート
- ・集中化されたアプリケーションやオペレーティングシステムソフトウェアによって論理的なアクセスコントロールに影響を及ぼしているコーディネート活動
- ・情報サービス部門内だけでなくサービスのユーザ部門にもセキュリティ認識とトレーニングを提供する

組織の施設内で人目から遮られたスタッフのための自動販売機，管理サービスの実施がある
セキュリティサービス契約内容，更新，交渉がある
侵入テストの手続と結果
- ・物理的な侵入テストシナリオを調整する
- ・ベンダとローカルの監督官庁によって物理的な侵入テストを調整する

健康，安全，環境の規則に準拠している
継続性計画において物理的なセキュリティが扱われ，供給元施設上で類似した物理的なセキュリティを保証する
導入セキュリティに必要な代替インフラ項目の具体的な存在：
- ・無停電電源装置（UPS）
- ・遠距離通信の代替ラインあるいは別ルート
- ・代替の水，ガス，空気調和，湿度装置

► 準拠性テスト:

スタッフはセキュリティと安全コントロールの必要性を認識し，理解する
配線用スペースは，許可されたもののみがアクセスできるよう物理的な安全策がとられ，ケーブルはできる限り地下あるいは安全な導管を通して配線してある
信号系は非常時ルートについて認識し，また非常時あるいはセキュリティ違反があった場合に何を行なうかを認識する
施設の他部分の中における信号系あるいは電話帳は，取り扱いに慎重を要する場所に設置しない
訪問者記録は適切にセキュリティ手続に従っている
あらゆる入出アクセスに対して確認手続が，必要とされる。観察による。
ドア，窓，エレベータ，ドック，空気穴，ダクトそして他のアクセス方法が認識される
コンピュータ室は分離され，鍵をかけられ，必要な基準で運用人員や保守要員だけにアクセスされる
施設スタッフはシフト交替し，適切な休日や休暇を取る
作業のタイムリーな実施のために保守手続と記録が存在する
2交替，3交替運用の方針と手続からの相違が報告される
構成，環境，施設の変更として物理的な計画が更新される
周囲のそして安全のモニタをしている設備と記録--フロアの下，上，上方，まわり--が維持される
危険な日用品が蓄えられない
アクセスコントロールの監査証跡がセキュリティソフトウェアあるいは主要な管理報告書に存在する
過去の緊急事態あるいは同じドキュメンテーションが追跡される
アクセスのあるスタッフは実際の従業員である
アクセスの主要な管理完全チェックがある
物理的なガード教育と周知が実施されている
セキュリティ結果，損失ビジネス，施設を復旧するのに要するコストに関する保険適用範囲とコストが存在する
鍵と論理的プロセスコントロールに対するアクセス変更を導入するためのプロセスが稼動中であり，知られている
環境は規制されたあるいは法定の要求に合う
アラーム保守記録は不適当に変えられることができない
アクセスコード変更とプロフィールレビューの頻度--ユーザと施設のかかわり合い--が文書化される

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:

類似した組織あるいは適切な国際的な標準／認められた産業の最適実務に対する施設管理をベンチマークする
建築図面とセキュリティ装置の物理的なレイアウト比較する
以下のことを決定する:

- 施設自体はシステムサービス施設表示せず，方向，駐車場サインなどによってこれを間接的に示す

(実証性テスト続き)

- ドアの数はローカル建築／保険法によって制限される
- 施設のロケーションは不適当なアクセスから乗り物や人々を守ために，十分な物理的な柵で守られる
- 安全なエリアに人々を案内しない流れを確かめるための通行の諸パターン
- ビデオをモニターすることとテープのレビューが十分である
- コンピュータ設備の設置場所がアクセス，熱，保守にふさわしい
- 非常時における水あるいは異質な要素に対して，十分な設備カバーが利用できる
- 保守記録からのアラーム効果と最新のアラーム訓練報告がレビューされている

温度，湿度，電気--上げられた床の上と下に関するテスト；異常が生じた際，結果として生じた調査／解決活動はどのようであったか
すべての錠と蝶番（部屋の内側にある蝶番）のチェック
バッジなしで歩き，同上のものがないことに関して照会されたかどうか決める
訪問者が施設を通って連れていったときの守衛／受付係の適用範囲レビュー
施設のセキュリティ侵入テスト

► 実証性テストの結果:

信号系，消火器，スプリンクラーシステム，UPS，排水，配線，可動性，定期的な保守の十分性
窓に対して：外部に目に見える資源やデータセンター内の「ショウケース」窓もないことを保証する
セキュリティ侵入テストの判定
登録，バッジ，付き添い，荷物検査，解放を含む訪問者テスト
訪問者バッジに対する訪問者記録の不一致
失ったバッジ／鍵カードの代用品と失った活用していない項目を含んでいる重要な管理報告に基づいたアクセスプロフィールと履歴のアセスメント
局所的な災害統計のレビュー
災害侵入シナリオを開発する
健康と安全の要求の人員と承諾の審査に対するベンダ契約がある
UPSのテストを行ない，結果が重大なデータ処理活動を維持するための容量と作業の要件を満たすことを確かめる
適切さのためにアクセス情報（ログ，テープ，記録）のテストが，ユーザと管理者によってレビューされる
手続をモニターしている近い場所の施設入口のテスト

DS13 運用管理

コントロール目標

1 処理運用手続と教育マニュアル
2 開始プロセスと他の運用文書
3 ジョブ･スケジューリング
4 標準ジョブ･スケジュールとの差異
5 処理の継続
6 運用ログ
7 遠隔運用

高レベルかつ詳細なコントロール目標

理解

面接対象者:

情報サービス部門の運用管理者
情報サービス部門の継続性計画管理者
情報サービス部門の上級管理者
情報サービス部門資源のユーザから選定したもの
ソフトウェアあるいはハードウェアの契約サービスか製品を提供しているベンダから選定したもの

収集すべき証拠資料:

ビジネス目的を達成するために情報システムの運用管理者と役割に関係する組織的な方針と手続
運用の役割，実行予想，ジョブスケジューリング，サービスレベル協定，オペレータ指示，スタッフローテーション，継続性計画，遠隔施設作業に関係がある情報サービス部門の方針と手続
スタートアップの一般的な機能，シャットダウン，作業負荷スケジューリング，標準，サービスレベル協定，緊急事態修復手続，異常な処理の応答，コンソールログ，物理的そして論理的セキュリティ，開発と本番のライブラリの分離，問題エスカレーション手続に対する運用指示
スケジュール，入力，処理時間，エラーメッセージ，異常終了指示，リスタート，問題上申手続，ジョブの前後オフサイトファイルを含んでいる主要なアプリケーションに対する作業指示の選び出されたサンプル

コントロール評価

評価視点:

以下にあげる証拠がある
- 実行したすべて処理，コールドスタート，リスタート，および復旧処理の完全性
- 初期プログラムロード（IPL）とシャットダウン手続の十分性

(評価視点続き)

・すべての要件の成功した完了を確かめるためのスケジュール完了統計
・ソースとオブジェクトの物理的，論理的な分離，テスト／開発／本番ライブラリ，ライブラリ間で移行するプログラムに対する変更コントロール手順
・以下にあげるものを含む運用活動に対するパフォーマンス統計，ただしこれらに限らない：
  ・ハードウェアと周辺装置の能力，使用とパフォーマンス
  ・メモリの使用とパフォーマンス
  ・遠距離通信の使用とパフォーマンス
・パフォーマンスが本番パフォーマンス標準，内部で定義されたパフォーマンス標準，ユーザサービスレベル契約責務と一致している範囲
・オペレーティング記録が維持され，保持され，そして稼動中の基準でレビューされる
・メンテナンスは適時にすべての設備に行なわれている
・オペレータはシフト交替され，休日と休暇をとり，そして能力を維持する

準拠性評価

準拠性テスト:

運用スタッフメンバは以下のことを認識し，理解する：
・責任ある運用の手続
・施設内のパフォーマンス予想--ベンダ標準，組織標準，ユーザとのサービスレベル協定
・リスタート／復旧手続に沿った非常時プログラムの固定
・運用を記録する要件と管理者レビュー
・問題上申手続
・シフト変更の連絡と内部シフトの責任
・開発プログラムから本番へ移行することに対する転換手順
・遠隔処理施設と中央処理施設との相互作用
・管理者に生産性改善機会を伝達することに対する責任

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

使用の適性を確かめるための運用パフォーマンス統計（設備と人員）のレビュー；類似した組織，ベンダ標準，適切な国際標準と同種の産業基準／最適実務との比較
限られた情報サービス部門の運用マニュアルのサンプルについてのレビュー，それらが方針と手続の要求を満たしているかどうかを決める
スタートアップとシャットダウンのプロセスドキュメンテーションの試験，手続がテストされ，定期的な基準でアップデートされるということを確かめるための経験
スケジュールに対するパフォーマンスの適切性と十分性を保証するための処理スケジュールの試験

► 実証性テストの結果:

ユーザを選択し，進行中の活動やサービスにレベル協定に関する運用パフォーマンスの十分性を確かめる

異常終了（ABENDS）をサンプルし，生じた問題の解決を決定する

オペレータトレーニング，シフトローテーション，休日／休暇の経験

正確さのためのコンソールログのサンプル，パフォーマンスの傾向，問題解決のための管理者レビュー--もし適用できるならば問題上申を評価する

サービスレベル協定責務満足を決めるためのユーザ

ベンダ提案につきすべての設備で完了されてきた予防保全手続

モニタリング

M1 プロセスのモニタリング

コントロール目標

1 モニタリングデータの収集
2 パフォーマンスの評価
3 顧客満足度の評価
4 管理者による報告

高レベルかつ詳細なコントロール目標の監査手続

理解

► 面接対象者:

CEO (最高経営責任者)
CIO (情報戦略統括役員)
上級内部監査役員
情報サービスの上級管理者と品質管理者
外部監査人の上級管理者
選出した情報サービス部門のユーザ
適用可能な場合, 監査委員会のメンバ

► 収集すべき証拠資料:

実績の計画, 管理, モニタリング, および報告に関する組織の方針と手続き
実績改善提案やレビューの頻度の確立, 実績のモニタリングや報告に関する情報サービス部門の方と手続き
次の事項を含む情報サービス部門の活動報告書, ただし次の事項のみに限定されるわけではない:部報告書, 内部監査報告書, 外部監査報告書, ユーザ報告書, 顧客満足度調査書, システム開発計画／状況報告書, 監査委員会議事録, その他情報サービス部門の資源利用に関する評価
資源グループ各々の成果物を伴う情報サービス部門の計画文書と計画に対する実績

コントロール評価

► 評価視点:

情報サービス部門の資源をモニタリングするためのデータは適切か
主要実績指標(KPI)と重要成功要因(CSF)を情報サービス部門の目標レベルに対する実績の測定に使用しているか
情報サービス資源利用の内部報告 (要員, 施設, アプリケーション, 技術, データ) は十分か
情報サービス資源実績報告に対して管理者によるレビューが行われているか
信頼でき, 有益なフィードバックを提供するための適時なモニタリング・コントロールが存在するか

(評価視点続き)

品質管理, 内部監査, 外部監査の改善要請に対する組織の対応は適切か
目標とする実績改善提案と結果が存在するか
組織内の全グループの決められた目標に対する組織の実績が発生しているか
顧客満足度分析がなされているか
外部監査人, 監査委員会, 組織全体の上級管理者等のような, ユーザ以外の者への実績報告の信頼性, 利用可能性は十分か
性能の低下や例外の発生を認識した時に迅速に対応できるように,適時な報告がされているか
業務の実施のために確立されている方針や手続きに対する報告は十分か (例えば, 実績報告)

► 準拠性テスト:

データ運用のモニタリング報告書があるか
運用モニタリングの報告書を管理者がレビューし, 改善活動を率先しているか
従業員は性能のモニタリングに関する方針と手続きを認識し理解しているか
以下に関する内部報告の質と内容:
- ・実績のモニタリング・データの収集
- ・実績のモニタリング・データの分析
- ・資源性能データの分析
- ・性能問題についての管理者の行動
- ・顧客満足度調査の分析

上級管理職は性能のモニタリングの報告に満足しているか

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:

性能モニタリングを同様な組織や適切な国際標準／確認されている業界での最良の実績値と比較評する
モニタリング中のプロセスにあるデータの適切性のレビュー
すべての情報サービス機能の領域での性能の計画と実績のレビュー
すべての情報サービス機能の領域での顧客満足度の期待値に対する実績
性能目標改善提案の遂行度合いの分析
マネジメント勧告の実施レベルの分析

► 実証性テストの結果:

情報システム組織に存在する監視要員の, 能力, 権限, および独立性

M2 内部統制の妥当性の評価

コントロール目標
1 内部統制のモニタリング 2 内部統制の適時な運用 3 内部統制レベルの報告 4 運用セキュリティと内部統制の保証

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

CEO (最高経営責任者)
CIO (情報戦略統括役員)
上級内部監査役員
情報サービスの上級管理者と品質管理者
外部監査人の上級管理者
選出した情報サービス部門のユーザ
適用可能な場合, 監査委員会のメンバ

収集すべき証拠資料:

内部統制についての計画, 管理, モニタリング, および報告に関する組織の方針と手続き
レビューの頻度, 内部統制のモニタリングや報告に関する情報サービス部門の方針と手続き
次の事項を含む情報サービス部門の活動報告書, ただし次の事項のみに限定されるわけではない:部報告書, 内部監査報告書, 外部監査報告書, ユーザ報告書, システム開発計画, 状況報告書, 監査委員会議事録, その他情報サービス部門の内部統制に関する評価
運用上のセキュリティと内部統制の保証に関して, 情報サービス部門が特に定めた方針と手続き

コントロール評価

評価視点:

情報サービス部門の内部統制をモニタリングするためのデータは適切か
情報サービス部門の内部統制データの内部報告は十分か
情報サービス部門の内部統制に対して管理者によるレビューが行われているか
信頼でき, 有益なフィードバックを提供するための適時なモニタリング・コントロールが存在するか
品質管理, 内部監査, 外部監査の改善要請に対する組織の対応は適切か
目標とする内部統制改善提案と結果が存在するか
内部統制の決められた目標に対する組織の実績が発生しているか

(評価視点続き)

内部統制のエラー，矛盾，および例外事象に関する情報が体系的に保存され管理者に報告されているか

外部監査人，監査委員会，組織全体の上級管理者等のような，ユーザ以外の者への内部統制報告の信頼性，利用可能性は十分か

内部統制の欠点や例外事象を認識した時に迅速に対応できるように,適時な報告がされているか

業務の実施のために確立されている方針や手続きに対する内部統制報告は十分か (例えば，内部統制報告)

► 準拠性テスト:

内部統制のモニタリング報告書があるか

内部統制報告書を管理者がレビューし，改善活動を率先しているか

従業員は内部統制のモニタリングに関する方針と手続きを認識し理解しているか

以下に関する内部報告の質と内容:

- ･内部統制のモニタリング･データの収集
- ･内部統制の適合性
- ･内部統制問題についての管理者の行動
- ･運用セキュリティと内部統制の保証

上級管理職はセキュリティおよび内部統制のモニタリングの報告に満足しているか

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:

内部統制評価を同様な組織や適切な国際標準／確認されている業界での最良の実績値と比較評価する

モニタリング中のプロセスや内部統制報告の中にあるデータの適切性のレビュー

プロセスの所有者にとって十分な適用範囲とさまざまなレベルの詳細を明確に保証するための組織体と情報サービス部門の内部統制レビューフレームワークの確認

すべての情報サービス機能の領域での内部統制の計画と実績のレビュー

内部統制目標改善提案の遂行度合いの分析

監査委員会が内部統制に関する報告に満足しているかをレビュー

マネジメント勧告の実施レベルの分析

► 実証性テストの結果:

内部統制報告の可能な付加的な領域が情報サービス，監査，管理者，外部監査人および規制団体などと矛盾がないこと

情報システム組織に存在する内部統制レビュー要員の，能力，権限，および独立性

M3 独立した保証の確保

コントロール目標

1 ITサービスについての独立したセキュリティおよび内部統制の認証／認定
2 第三者機関のサービスプロバイダについての独立したセキュリティと内部統制の認証／認定
3 ITサービスについての独立の有効性評価
4 第三者機関のサービスプロバイダについての独立の有効性評価
5 法律と規則の要件と契約上の誓約の独立の準拠性保証
6 第三者機関のサービスプロバイダについての法律と規則の要件と契約上の誓約の独立の準拠性保証
7 独立的保証機能の能力
8 積極的な監査の関与

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

CEO (最高経営責任者)
CIO (情報戦略統括役員)
情報サービスの上級管理者
上級内部監査役員
外部監査人の上級管理者
独立した保証機関の上級管理者

収集すべき証拠資料:

組織全体の組織図と方針および手順のマニュアル
独立的保証のプロセスに関する方針と手続き
ITサービス提供者の契約書／サービスレベル合意書
適切な法的および規制的要件と契約条項
独立的保証機関の免許状／契約書，予算書，以前の報告書および業績履歴書
独立的保証機関の職員の経験と継続教育の履歴
以前の監査報告書

コントロール評価

評価視点:

独立的保証の免許状／契約書は，充分なレビュー範囲を確保するのに適切に確証／執行できるものであるか (例えば，証明書／認定証，有効性評価，適合性評価)
独立性の証明書／認定証は重要な新しいITサービスを導入する前に取得しているか

(評価視点続き)

ITサービスの独立性の再証明書／再認定証は導入後に定期的な周期で取得しているか
独立性の証明書／認定証はITサービスプロバイダを使う前に取得しているか
独立性の再証明書／再認定証は定期的な周期で取得しているか
ITサービスの有効性の独立性評価は定期的な周期で行っているか
ITサービスプロバイダの有効性の独立性評価は定期的な周期で行っているか
情報サービス部門が法や規制要件や契約の履行を遵守しているかについての独立した検証が，定期的な周期で行われているか
第三者機関のサービスプロバイダが法や規制要件や契約の履行を遵守しているかについての独立した検証が，定期的な周期で行われているか
独立した保証機関の職員は，能力があり，適切な職業的標準に従って作業を遂行しているか
継続的専門教育プログラムで独立した保証機関の職員は技術能力を養うようになっているか
管理職はITサービスにおける解決策を決定する前に積極的に監査必要性を検討しているか

► 準拠性テスト:

上級管理職は独立した保証機関の実績を承認しているか
重要な新しいITサービスを導入する前に独立性の証明書／認定証は包括的なものであり，完全でタイムリーなものか
ITサービスの独立性の再証明／再認定は導入後の定期的な周期で実行されており，また，それらは包括的なものであり，完全でタイムリーなものか
ITサービスプロバイダを使う前の独立性の証明書／認定証は包括的なものであり，完全でタイムリーなものか
独立性の再証明／再認定は定期的な周期で実行されており，また，それらは包括的なものであり，完全でタイムリーなものか
ITサービスの有効性の独立性評価はルーチンサイクルで実施され，定期的な周期で実行されており，また，それらは包括的なものであり，完全でタイムリーなものか
ITサービスプロバイダの有効性の独立性評価はルーチンサイクルで実施され，定期的な周期で実行されており，また，それらは包括的なものであり，完全でタイムリーなものか
情報サービス部門が法や規制要件や契約の履行を遵守しているかについての独立した検証が定期的な周期で実行されており，また，それらは包括的なものであり，完全でタイムリーなものか
第三者機関のサービスプロバイダが法や規制要件や契約の履行を遵守しているかについての独立した検証が定期的な周期で実行されており，また，それらは包括的なものであり，完全でタイムリーなものか
独立した保証部門の報告書は，調査結果，結論，勧告に関して適切か
独立した保証部門は，有効な仕事の遂行に必要な技術や知識を有しているか
ITサービスにおける解決策を決定する前に積極的な必要性が検討されているか

実証性テスト:

独立した保証機関の検証活動を同様な組織や適切な国際標準／確認されている業界での最良の実績値と比較評価する

詳細な検証項目:

- 独立的保証の免許状／契約書を，実行された検証活動と検証する
- 証明書／認定証の妥当性や適時性を決定する
- 証明書／認定証の妥当性や適時性を決定する
- 有効性評価の妥当性や適時性を決定する
- 法や規制要件や契約の履行を遵守しているかについての検証の妥当性や適時性を決定する
- 独立した保証部門の職員の能力を検証する
- 積極的な監査必要性を検証する

実証性テストの結果:

独立した保証の検証活動による付加価値

独立した保証計画および予算と比較した業績の計画に対する実績

積極的な監査の必要性についての範囲と適時性

M4 独立的監査の提供

コントロール目標
1 監査規程 2 独立性 3 専門家としての倫理と基準 4 能力 5 計画 6 監査業務の実施 7 報告 8 フォローアップ活動

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

CEO（最高経営責任者）
CIO（情報戦略統括役員）
上級内部監査役員
情報サービスの上級管理者と品質管理者
外部監査人の上級管理者
適用可能な場合，監査委員会のメンバ

収集すべき証拠資料:

組織全体の組織図と方針および手順のマニュアル
組織全体の活動方針の規範
独立監査のプロセスに関する方針と手続き
監査規程，業務命令書，方針，手続きと標準，以前の報告書，および監査計画
外部監査の意見書，レビュー，および監査計画書
内部監査員の経歴と継続教育の履歴
監査リスクの評価，予算および業務履歴
適用可能な場合，監査委員会の議事録

コントロール評価

評価視点:

適用可能な場合，監査委員会が適切に設立され，定期的に会議が行われていること
内部監査組織が適切に設立されていること

(評価視点続き)

外部監査が監査計画の仕上げに貢献していること
専門家に適用される行動規範は十分に厳守されていること
監査人の独立性は，署名された利害関係のないことの宣誓書によって確認すること
監査計画はリスク評価の方法論に基づいて計画され，全体的に十分であること
監査は適切に計画され，監督されていること
監査証拠は発見事項や結論を裏付けするに十分であること
継続専門教育プログラムは監査人の技術的能力向上に役立っていること
監査人は能力を持ち，専門家としての監査基準に基づいて業務を遂行していること
管理者に対して監査発見事項を適切な報告するプロセスがあること
すべてのコントロール上の課題に対するフォローアップは適宜行われていること
監査対象領域には情報システム監査のすべての領域が含まれること (つまり，全般統制と業務処理統制，システム開発のライフサイクル，採算性，経済性，効率性，有効性，監査の積極的なアプローチ，など)

準拠性の検証

► 準拠性テスト:

上級管理者が進行中の独立監査部門の業務遂行を承認していること
上級管理者の態度が監査規程と矛盾していないこと
内部監査は専門家としての基準と比較評価されていること
監査人の担当は独立性と十分なスキルが保証されていること
監査人の職業専門家としての信用が常に改善されていること
監査報告書の内容は勧告に関して適切であること
改善実施の時期をまとめたフォローアップ報告書が存在すること

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:

監査部門を同様な組織や適切な国際標準／確認されている業界での最良の実績値と比較評価する
詳細な検証項目:

- 監査計画に周期的で継続的なレビューが記述されていることを検証する
- 監査がビジネスの成功とIT業務計画に貢献している
- 監査部門の証拠が結論と勧告を裏付けしている
- 監査発見事項が伝達され，リスクの軽減または有利になる好機となっている
- 監査の勧告が利益の実現をともなって導入されている

► 実証性テストの結果:

監査勧告のコスト対効果
監査計画および予算と比較した業績の計画に対する実績
外部監査, 内部監査間の統合の度合い

付録IV － 監査プロセス

（当監査プロセスは，米国ISACAのNational Capital Area 支部により作成された。）

以下に示すフローチャートでは，単一の***コントロール目標***達成のために，履行すべきステップの各々について検討がなされている。そこではステップの目標の概要を述べ，監査人が次のステップに進む前に何を達成しておくべきかを示す。最後に，フローチャートは，各ステップで取られるべき情報収集と意思決定プロセスの図を示す。

多くの目標がユニークであるので，我々はこのテンプレートを厳しいルールを課して使用することは薦めない。このテンプレートは，監査業務の各フェーズに関する正確な概念フレームワークを示すので，ガイドとして有用と考える。 統一用語集は，テンプレートの後に示されている。 テキストでは，定義された用語は***イタリック***で示されている。

識別/文書化 監査ステップ：

ステップの目標－識別/文書化という監査ステップの目標は，***コントロール目標***によってカバーされた***タスク***や，ISの管理者がそれ *(**コントロール目標**)* をコントロールしていることをどのように確信しているかを監査人が精通する様になることである。これには，その***タスク***を遂行している個個人，プロセス，場所，それ *(**タスク**)* をコントロールする為の***表明された手続***の識別が含まれる。

ステップの期待成果物－識別/文書化の監査ステップの終了に際して，監査人は以下について明らかにし，文書化し，検証しておくべきである。

- ***コントロール目標***によってカバーされる***タスク***の実行者
- ***タスク***の実施場所
- ***タスク***の実施時期
- ***タスク***実行時の***入力***
- ***タスク***からの期待される***出力***
- ***タスク***実行の為の***表明された手続***

評価 監査ステップ：

ステップの目標－評価という監査ステップの目標は，***表明された手続***を評価し，手続が効果的なコントロール構造を提供するかどうかを判定することである。手続は，明らかにされた基準，業界標準慣行，監査人の判断に照らして評価されなければならない。効果的なコントロール構造は，コスト効果があり，***タスク***の実行と***コントロール目標***の達成という合理的保証を提供する。

ステップの期待成果物－評価という監査ステップの終了に際して，監査人は以下を完了させておくべきである。

- 手続への適用可能性に関して法律，規制，組織基準を評価する
- それら *(**表明された手続**)* はコスト効果があり，***タスク***の実行と***コントロール目標***の達成という***合理的保証***を提供しているかどうかを確認するために，***表明された手続***を評価する
- 弱い手続を支援するために用いられる***補完コントロール***を評価する
- ***表明された手続***と***補完コントロール***が一緒になって効果的なコントロール構造を提供しているかどうかを結論付ける
- 準拠性テストが適切であるかどうかを明らかにする

準拠性試査 監査ステップ：

ステップの目標－準拠性試査という監査ステップの目標は，規定されたコントロールに対する組織の準拠性を分析することである。***実際の手続***と***補完コントロール***は，***表明された手続***と比較されなければならないし，文書レビューとインタビューは，コントロールが適切でありそして一貫して適用されているかどうかを決定するために実施されること。準拠性試査は，効果的であると考えられる手続きに対してのみ実施される。

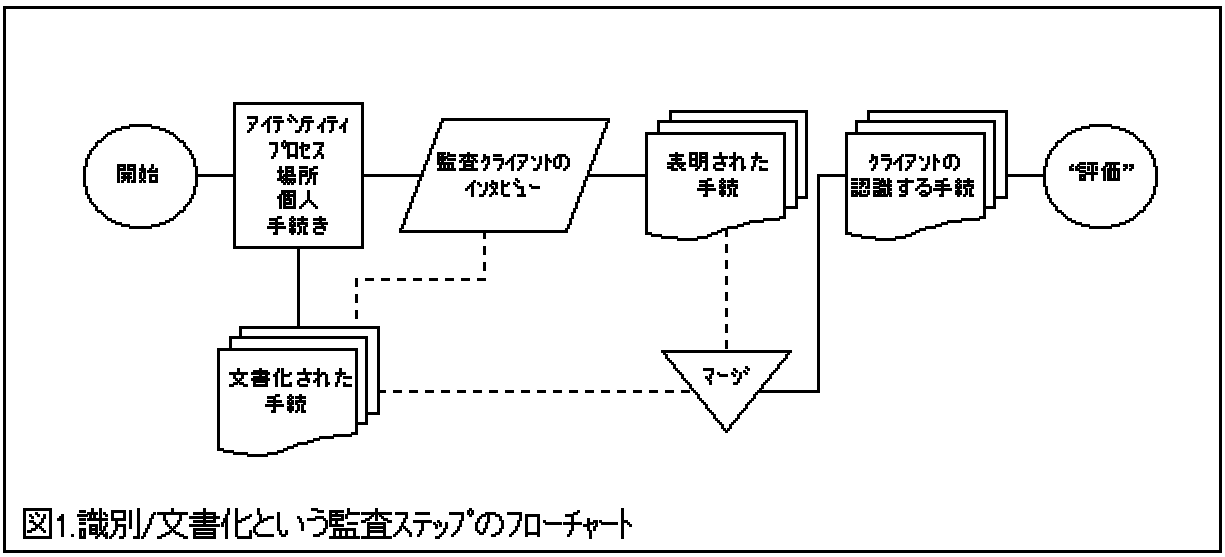


図1.識別/文書化という監査ステップのフローチャート

付録IV　－　監査プロセス

ステップの期待成果物－準拠性試査の監査ステップの結論で，監査人は上で明らかにされた手続への組織の準拠性を文書化し，組織は***表明された手続***と***補完コントロール***を適切かつ一貫して適用してきたか否かを結論付けておくこと。監査人は準拠性のレベルに基づいて，コントロール・プロセスが適切であるという保証を与えるのに必要な実証性テストの水準を決定すること。

実証性テスト　監査ステップ：

ステップの目標－実証性テストという監査ステップの目標は，必要なデータ・テストを実施することであり，それにより，所与の***ビジネス目標***の達成について，マネジメントに対し最大限の保証を与えるか，または一切保証を与えないことである。

ステップの期待成果物－実証性テストという監査ステップの終了に際して，監査人は所与の***コントロール目標***が達成されつつあるか否かを決定するために，***タスク***の成果物に関し十分なテストを実施しておくべきである。 重要な実証性テストは，以下の場合に実施すべきである。

- コントロール対策が適切でない
- コントロール対策が不充分なものとして評価されてきている
- コントロール対策が適切にかつ一貫して適用されてこなかったことを，準拠性試査が示している

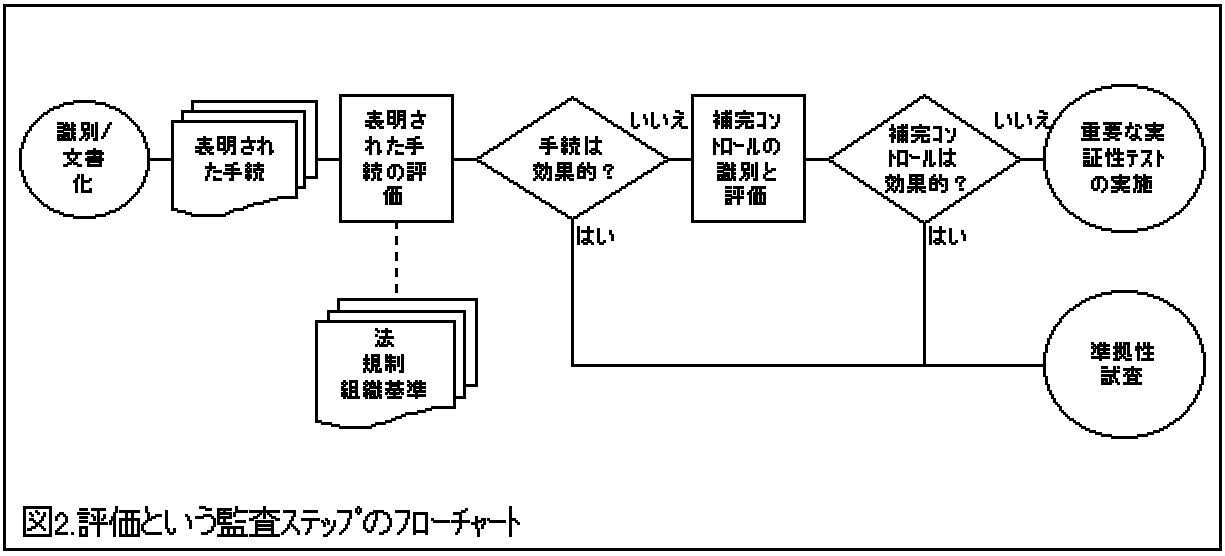


図2.評価という監査ステップのフローチャート

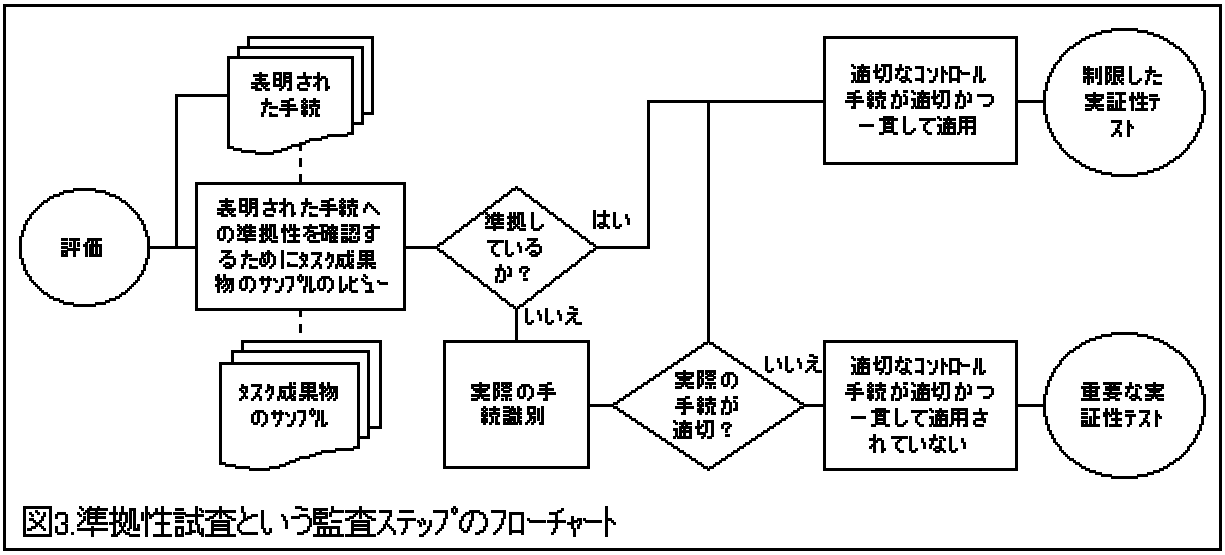


図3.準拠性試査という監査ステップのフローチャート

付録IV　－　監査プロセス

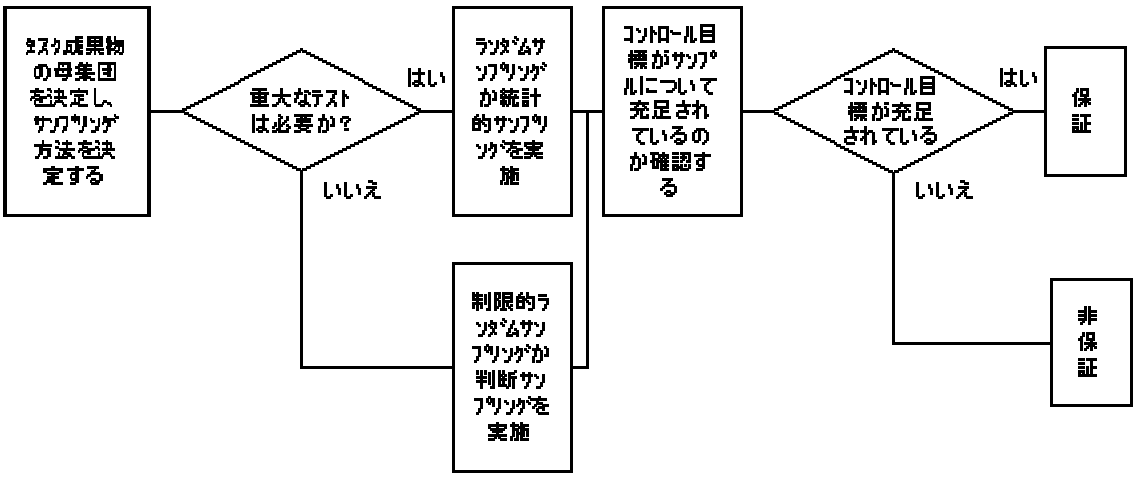


図4.実証性テストという監査ステップのフローチャート

付録IV　－　監査プロセス

用語集:

実際の手続－実際の手続とは，監査目標を履行するために組織によって実施されている手続のことである。 実際の手続は，監査の準拠性試査の局面で識別される。

補完コントロール－補完コントロールとは，テストされるコントロール目標に直接的に関与しない追加的なコントロールのステップまたは手続のことである。しかし，その（補完コントロール）存在がコントロール目標に直接関与するコントロールを強化するのに役立つ。補完コントロールは，監査業務の準拠性試査の局面で識別される。補完コントロールは，表明されたコントロールの有効性が疑わしいときのみ積極的に要求される。

コントロール目標－組織の為に制定された手続きにより期待される成果を示す。ISの立場からすれば，コントロール目標は，実施される監査業務の範囲を分類し定義するために用いられる。

合理的保証－特定のコントロール目標を達成する為に制定された手続の適切性を評価する為の標準。合理的保証は，情報に基づいた意見を展開する為の判断，知識，経験の適用を含む。合理的保証により要求されることは，コントロールのシステムが効果的であること，但し過度に過重のかかるものであってはならないことである。合理的保証の標準は，また，コントロールのシステムがコスト対効果に優れていることである。

表明された手続－組織が確信するコントロールは適切で有り，コントロール目標が達成されつつあるという保証を与える為に遵守される。表明された手続は，経営者が確信することの具現化である。表明された手続は，文書化された手続と経営者が特定した非公式の手続の双方を含む。表明された手続は，監査ステップの識別/文書化フェーズの中において明らかにされ，準拠性試査の局面で実際の手続と比較される。

タスク－コントロール目標によってカバーされる一連の手続による期待成果物。タスクは，コントロール目標に保証を進展させたものである。

タスクのインプットとアウトプット－タスクの遂行に必要な，関連する，または実施結果としての製品，報告書，または情報。

付録Ｖ

ロバート･パーカー氏（元ISACA会長）は，特定のプロセスのみならず特定の問題へのCOBIT*フレームワーク*の適用例として，西暦2000年問題へ適用できる監査ガイドライン例を提示している。－西暦2000年問題は，コンピュータ･プログラムの日付フィールドに関して，最後の桁が“99”から“00”へ変わることに関連する潜在的な処理の困難さに関する問題である。

説明の意図は，すべてを網羅するのでは無く，むしろ監査ガイドラインを構築するためにCOBITフレームワークを使うテーマへのアプローチとしての有用さに置かれている。

2000年対応

コントロール目標

1 すべてのアプリケーション･プログラムが2000年対応済みであることを保証すること
2 すべてのハードウェアとシステム･ソフトウェアが2000年対応済みであることを保証すること
3 すべての計画が適切に2000年対応を監視し，必要なところでタイムリーに対応していることを保証すること

高レベルかつ詳細なコントロール目標の監査手続

理解

面接対象者:

CEO（最高経営責任者）
CIO（情報戦略統括役員）
情報サービス機能運営委員会の選ばれたメンバ
組織の2000年特別小委員会の議長
2000年に率先して対応する責任のある情報サービス機能の管理者
2000年対応を率先して実施し，配付する責任のある情報サービス機能の担当者
電子商取引アプリケーションに責任のあるユーザ

収集すべき証拠資料:

具体的な時期と予算計上されたコストを含む組織の2000年計画
組織の 2000年評価報告書
アプリケーション，システム･プログラム，ユーティリティーとハードウェア装置毎に分類された2000年対応に必要な取り組みに対する情報サービス機能による分析
ベンダの2000年対応の保証に関する情報と，もし未対応ならば，予想される対応可能日付
2000年対応の特別小委員会会議の議事録
産業界全体の問題（例えば，電子商取引）を取り扱う関連した業界イニシアティブ

コントロール評価

評価視点:

組織は，適切な目録を準備してITの利用に関してレビューを実施し，また，潜在的な特定の2000年問題を適切に評価していなければならない。
組織は，システムが 2000年に対応することを保証するための計画を策定していなければならない。 また，完全に対応するために十分な時間を確保していなければならない。
組織は，既存システムを評価するために，具体的な計画を策定しなければならない。但し，そのシステムは，2000年対応とさせる為に修正を可能にさせる文書やソースコードが不充分である可能性がある。
組織は，供給者と電子的に取引（EDI,EFIなど）しており，そして彼らに適切な保証を含む2000年対応を要求するか否かに対処すること。
現存する文書の品質は，組織の2000年対応を可能ならしめるに十分であること。

(評価視点続き)

オペレーティング･システムと他のソフトウェアが 2000年対応を保証されていること。
組織は，システム設計，特に保存方針において ’99’ をデフォルトとして使用してきている (即ち，保存ファ
イルの保存を非削除にするために ’99365’ を指定)。
組織は，すべての新しいソフトウェアが2000年対応を保証されていることを要求する方針を採用していなければならない。
組織は，ソフトウェア･ライセンス契約で，2000年のテストを行なう代替サイトでそのソフトウェアの使用が許可されていることを保証しなければならない。
組織は，妥当性テストや計画された2000年対応イニシアティブを保証し，要求された時間内で完了させるための十分なスキルを持たなければならない。
組織は，2000年プログラムの実行を支援するためのソフトウェア製品を取得し，その妥当性検査を実施していなければならない。
組織は，2000年計画を完了するために外部資源に依存しているか，または今後依存するであろうし，そのような資源が既に契約下にある場合もある。
組織の 2000年計画は，コンピュータにより制御されている装置，例えば，ドア，アラーム，エレベータ，セキュリティ･コード，パス，ファクシミリ等も対象としていること。
組織は，現在の 2000年計画とあらゆる 2000年イニシアティブの状況から派生する「増大する心配」の問題を回避しなければならない。
組織は，組織の現在の 2000年計画とあらゆる 2000年イニシアティブの状況において生ずる組織管理の報告形態の問題を回避しなければならない。

準拠性評価

準拠性テスト:

アプリケーション，ユーティリティー， APIなどの目録が完全かつ正確であり，さらに2000年対応の状態が正しいこと。
2000年計画は完全であり，合理的であり，達成可能であり，そして適切に管理されていること。
サプライヤとの電子的インタフェースが2000年に対応していること。
組織が2000年対応を行なうのに必要となるすべてのプログラムを評価し，変更し，テストすることを可能ならしめる為に，ドキュメンテーションが適切であること
製造業者，ベンダ，その他の供給業者は，彼らの製品が2000年対応であること，さらに維持されたそのような保証の記録が存在することを証明しなければならない
2000年対応の保証製品に対して，組織は，通信を含む正式な/通常の処理環境下で適切なテストを実施していなければならない
デフォルト'99'の使用が，適切に取り扱われていること
組織の方針，手続，標準が 2000年要求を反映し，かつそれに準拠していること
現在のすべてのソフトウェアとハードウェアのライセンス契約は，2000年対応を明細に記述していること，および／または，ベンダ／供給者によって2000年対応の完了目標期日が指定されていること
組織は，組織の2000年イニシアティブをサポートするスキル保有を保証するために，すべての情報サービス部門の要員に十分な訓練期間を考慮していること
ソフトウェア･ライセンス契約により，組織が第一の認可場所以外のサイトで 2000年テストを実施できるようになっていること
組織の2000年イニシアティブは，完全なシステム･テストを含めて適切なテストと検証を実施できること。さらに，リモート処理と通信環境のシミュレーションの実施とテストの管理ができる適切なリモート･サ

イトが確保されていること

(準拠性テスト続き)

計画は，コンピュータ･システムに加えて装置を含んでいること

計画は，2000年の後に組織がその正規のビジネス活動を中断すること無く継続できるようになっていること

► 実証性テスト:

類似した組織あるいは適切な合理的な基準に対して，2000年に関する計画/イニシアティブ/ 現状とのベンチマークを実施する

見積り時間，与えられた資源，利用できるスキル，計上された予算の評価を含めて，種々の2000年イニシアティブについて詳細にレビューする

2000年対応の程度を評価する為に，ベンダと供給元との契約をレビューする

組織の2000年要求に応ずる為に，組織の2000年テストをレビューし，個々のシステムの対応を評価する

2000年の外部依託契約をレビューし，契約条件と成果物を評価する

► 実証性テストの結果:

非現実的か，野心的過ぎる2000年に対する計画とイニシアティブ

2000年に対する不十分な投資/資源割り当て/人員/スキル

2000年要求での不十分な，または不適切な契約の締結

2000年対応のために改善されたシステムとアプリケーション･プログラムに対する不十分なまたは不適切なテスト

2000年対応の為にベンダの供給したソフトウェアに関して，不十分な，または不適切な契約条項，条件，時期

2000年対応であることを「ベンダ保証」された第三者機関ベンダのソフトウェアに対する不十分な，または不適切なテスト