「システム管理基準追補版改訂案」に対する意見募集結果の概要及び具体的な修正内容

パブリックコメントに対してお寄せいただいた意見と、提出意見に対する考え方は以下のとおりです。皆様の御協力に厚く御礼申し上げます。

No.	提出意見	提出意見に対する考え方
1	この改訂は情報処理技術者試験、特にシステム監査に高い影響を及ぼすので、周知を十分に行ってほしい。	御意見いただきありがとうございます。今後の周知を図ってまいります。
2	参考文献をなくした理由をお示し頂き度。	御意見いただきありがとうございます。参考文献につきましては、本文中の必要な箇所（１章５ページなど）に示しておりますので、あえて一覧で表示しておりません。
3	以下、意見を行う。 ・該当箇所 全体的に（※記述が無いが、あった方が良いと思われた事についての意見） ・意見内容 CISO（最高情報セキュリティ責任者）についての記述が無いように思われるのであるが、CISOについての記述はあった方が良いのではないかと考える。 ・理由 CISOについて担当が決まっている方がISMS・ISO 27000シリーズ等と親和性が高いと思われ、ITガバナンスにも有用と思われるので。 少なくともその概念についての提示を行い、CISOについての担当者を決めておく、という意識付けをしておいた方が望ましいと考える。 であるので、少し触れるくらいでもよいのであるが、情報セキュリティあるいはCIOの職務について触れる際に、CISOについての記載も行った方が良いのではないかと考える。	御意見いただきありがとうございます。本追補版は、「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準」（以下「実施基準」という。）とシステム管理基準及びシステム監査基準（以下「システム管理基準等」という。）との関係を説明することを目的としております。御意見につきましては、情報セキュリティ管理基準等を参照いただくことを前提としておりますので、本追補版では特に記載をせず、原案のとおりとさせていただきます。
4	「IT基盤」と「IT全般統制の評価単位」について、実務者にわかり易いよう、かつ一貫性ある説明にして欲しい（関連用語の整理） 「IT全般統制の評価単位」は、実務の場面で新任者に誤解されやすい。具体的には、（IT全般統制の評価単位＝IT基盤の単位）あるいは、（IT全般統制の評価単位＝システムの単位） などと単純にとらえられ、誤解されやすい。このように理解されると「IT全般統制の評価単位」が必要以上に多くなり、その結果、評価実務に大きな負担となる。 「IT全般統制の評価単位」は、このように単純に決めるものではなく、財務諸表の信頼性確保の観点でリスクを想定→関連する業務プロセス→ＩＴとのかかわり（例：以下４点） ・アプリケーション・システム ・IT基盤 ・ITに関与する組織（利用部門、管理部門、業務委託先） ・ITの管理や利用のルール方針　など などによって、決めるものであると理解している。 今回の見直しでは、付録の参考例が整理され、IT基盤質問書が追加されるなどが行われ、わかり易くなっている。 しかし、追補版全体で関連する説明個所（付録、本文、図表）が複数個所に分散されているため、結果として、読者が理解し易いような一貫性のある説明になっていない可能性がある。 （下記該当箇所参照） 追補版の活用が進み、新任者を含め実務担当者が容易に理解し実務を継続できるよう、以下の用語について1か所でまとめたうえで、相違点を整理して欲しい。 「IT基盤」「IT統制」「IT全般統制」「組織」「ルール方針」「IT全般統制の評価単位」など ■該当箇所　※例えば、説明箇所ごとに「IT基盤」が指す範囲が微妙にずれているため混乱する読者が出る可能性ないか 第１章　P03（イ）IT基盤の概念 第２章　P12　図表２．１-３ 財務報告とIT統制との関係　の左下　IT基盤の説明 第３章　P26-27 図表３．２-１ ITに関して把握すべき内容の例 ・IT基盤と組織区分の相違 ・組織区分とIT基盤（IT全般統制）が一致しない場合 など	御意見いただきありがとうございます。本追補版は、実施基準とシステム管理基準等との関係を説明することを目的としており、両基準の変更に合わせた対応にとどめております。図表Ⅱ１－３については、御意見を踏まえ、IT基盤が指す範囲は原案に記載したものに限定されるものではないため、「データベース」を「データベース等」とするなど所要の修正をさせていただきましたが、それ以外は原案のとおりとさせていただきます。 なお、用語の説明については、前後の文脈で強調する部分が異なるため、原案のとおりとさせていただきます。

No.	提出意見	提出意見に対する考え方
5	付録2-1　IT基盤質問書（例）の記述例の一部修正と拡充してはどうか。 IT基盤質問書（例）の最後にある「４．評価対象とするITに係る全般統制とその評価単位の識別」の表の１行目、最右列「評価単位」に、記載してある「情報システム部」は、わかりづらいので、評価単位を識別するような名称（例：評価グループ０１、評価単位Ａ　など）にしてはどうか。 また、記載例が、１行（販売管理システム）だけでは少しわかりづらいので、売掛金管理システム、会計システム（cf.第３章　P32）なども記載し立体的な説明になっていると読者に理解し易いのではないか。 この表は、恐らく、最右列「評価単位」（＝IT全般統制の評価単位）を整理するための表であり、その前提として、判断要素（関連する業務プロセス、評価対象とするITアプリケーション・システム、IT基盤、ITに関与する組織　など）を左側に整理し、かならずしも、IT全般統制の評価単位が、システムの単位と一致しない様子を整理するための表であると推測する。 該当箇所 付録2-1　IT基盤質問書（例）　４．評価対象とするITに係る全般統制とその評価単位の識別	御意見いただきありがとうございます。御意見のような修正を行いますと評価グループや評価単位のイメージが把握しにくいと考えられますので、イメージを掴みやすい表現にする観点から、原案のとおりとさせていただきます。 なお、各社の状況に応じて読み替えて活用いただくことは差し支えありません。
6	重要な用語についての解説拡充を希望する（RCM：リスク・コントロール・マトリクス、他） 付録２のタイトルにもなっている「…リスクコントロールマトリクス（RCM）の例」は、付録2-2の各表タイトルでは「XXX評価記述書」なっている。 暗黙的に（RCM＝評価記述書）と説明しているため、内部統制評価実務に携わる担当者や新任者が混乱する可能性はないだろうか。 個人的には、 「評価記述書」は、RCMに整理した各統制目標（統制項目）ごとに評価を行い、その評価結果を記述した文書（RCMに評価を追加した文書）のことを指すものと理解していたのだが、これが正しい理解かどうかは自信が無い。 （明確に定義されている文書が探せず困っている。追補版を初めて見て、IT統制の参考にする読者も同様ではないだろうか） 追補版での想定（定義）が、 RCM　＝　リスクと統制（コントロール）の対応　＝　評価記述書 としているのであれば、その旨、用語の整理をして欲しい。	御意見いただきありがとうございます。いただいた御意見を踏まえ、次のとおり修正させていただきます。 「IT全社的統制評価記述書（例）」を「IT全社的統制リスクコントロールマトリクス（例）」に修正。 「IT全般統制評価記述書（例）」を「IT全般統制リスクコントロールマトリクス（例）」に修正。 「IT業務処理統制評価記述書（例）」を「IT業務処理統制リスクコントロールマトリクス（例）」に修正。

No.	提出意見	提出意見に対する考え方
7	リスクコントロールマトリクスの利用方法（付録２　P3）の説明内容は改善が必要ではないか 「２．リスクコントロールマトリクスの利用方法」（丸1-丸6）をあらためて読むと、意味が通じにくいところがある。 この部分では、付録2-2の表（３種類の　XXX評価記述書（例））の利用方法（記入・活用方法）を説明しているのだと思うが、説明と図表の内容が若干かみ合っていないように感じる。 そもそも この「２．リスクコントロールマトリクスの利用方法」の部分は、３種類のうちの２種類（IT全社統制、IT全般統制）の評価記述書の説明ではないだろうか。 ３種類目の「IT業務処理統制の評価記述書」の説明は、「１．リスクコントロールマトリクスの項目」の部分で説明されているため、（暗黙的にそのことが説明されている）現状では、読者が混乱する可能性はないか。 例えば、以下のように、現在の内容を整理修正してはどうか。 見直し案-1 タイトル「２．リスクコントロールマトリクスを使った利用方法」 →「２．リスクコントロールマトリクスを使った評価方法（IT全社統制、IT全般統制）」 (1)RCMの作成・見直し（概要） 1. RCMの作成・見直しの場面では、まず、リスクを記入する。 2. 統制目標欄には、実施している（構築を予定している）統制項目を記入して、関連する項目についても、リスクコントロールマトリクスに記入していく。 3. 統制を整備する場合には、候補となる統制項目をリストアップして、リスクの低減が図れる最適な統制項目を選択する。 (2)RCMを使った評価方法 1. RCMに列挙した統制項目の評価を進めるに際し、あらかじめ統制目標（統制項目）の評価手続を記入しておく。 2. 最初に、統制目標（統制項目）ごとに、統制の状況を把握し、どのような評価項目と関係するのかを概観する。 3. 統制項目を評価する場合には、想定したリスクに対して、選択した統制項目がリスクを低減しているかを評価する。 4. 評価した結果（統制目標が有効に機能しているかどうか）について記録に残す。 仮に、有効でないと判断した場合には、その旨を検出事項に記入し評価結果として記録に残す。後日、改善検討のインプットにする。 見直し案-2 タイトル「１．リスクコントロールマトリクスの項目」 →「１．リスクコントロールマトリクスを使った評価方法（IT業務処理統制）」 ※内容は、現状のままで良い（IT業務処理統制の評価記述書の説明になっている）と思うが、用語の一貫性や用語の説明が欲しい部分は、以下の１点 ・アサーション 説明文では「評価項目」となっているが、図表の列名は「アサーション」となっている。 （暗黙的に読み手に読み替え変換し理解を求めるようになっている）	御意見いただきありがとうございます。いただいた御意見を踏まえ、次のとおりとさせていただきます。 「①まず、リスクを記入する。 ②リスクに対する統制目標及び実施している（構築を予定している）統制の状況を記入して、関連する項目について、リスクコントロールマトリクスに記入していく。 ③統制の状況を把握する。IT業務処理統制の場合には、どのような評価要件（アサーション）と関係するのかを概観する。統制を評価する場合には、統制評価手続を記入して統制の評価を実施する。 ④統制を整備する場合には、候補となる統制項目をリストアップして、リスクの低減・統制目標の達成が図れる最適な統制項目を選択する。 ⑤統制を評価する場合には、想定したリスク及び統制目標に対して、統制の状況がリスクを低減しているかを評価する。 ⑥その結果を評価及び検出事項に記入し、低減されたリスクを右端の評価結果に記入する。」 また、本修正に伴い、付録２－２の１「評価項目」を「評価要件（アサーション）」とした上、説明文を次のとおり見直しています。 「評価要件（アサーション）：IT業務処理統制では、適切な財務情報を作成するための要件（評価要件）である網羅性、実在性、期間配分、権利と義務の帰属、評価、表示を記入。なお、財務諸表監査では、適切な財務情報を作成するための要件について、アサーションという用語を使用しており、実務でもアサーションが多く使用されていることから、アサーションと表記している。」
8	付録１　３（１）手作業による場合　の　最後の段落は、説明文の一部改善が必要ではないか。 理由 説明する内容が複雑なのでできるだけ簡潔に説明できれば良いと思うが、過度に省略されずぎていて読み手が具体的な内容を理解しにくいのではないか。 該当箇所 IT全般統制は、財務報告の虚偽記載に直接影響を及ぼすものではないが、IT業務処理統制が有効に機能していることを保証するので、IT業務処理統制ごとにアプリケーション・システムを検証することを軽減できる。この場合のサンプル件数は、例えば、付録図表１-１を参考にして選ぶことができる。 見直し案　※【】の部分を追加 IT全般統制は、財務報告の虚偽記載に直接影響を及ぼすものではないが、【IT全般統制をテストし、その有効性を証明することで間接的に】IT業務処理統制が有効に機能していることを保証するので、IT業務処理統制ごとにアプリケーション・システムを検証することを軽減できる。 この場合の【IT全般統制テストの】サンプル件数は、例えば、付録図表１-１を参考にして選ぶことができる。	御意見いただきありがとうございます。御意見を踏まえて改めて検討した結果、該当箇所を削除させていただきました。

No.	提出意見	提出意見に対する考え方
9	説明文の一部整理見直し必要ではないか。（ITを利用した内部統制の特性、長所と短所） 該当箇所： 第２章 P16 丸4）ITを利用した内部統制の長所と短所 理由： 特性、長所、短所 の整理が十分でないため、理解しずらい。現状では、短所の説明が２回記載されているように見えてしまう。 例えば、以下のように、現在の内容を整理してはどうか。 見直し案 タイトル 「丸4）ITを利用した内部統制の長所と短所」 →「丸4） ITを利用した内部統制の特性、長所と短所」 （特性） 情報システムにおいては、一旦適切な内部統制（業務処理統制）を組み込めば、意図的に手を加えない限り継続して機能する性質を有している。 （長所） 統制活動が自動化されている場合、手作業による統制活動に比べて迅速な情報処理が期待できるほか、人間の不注意による誤謬等の防止も可能となり、この結果として、内部統制の評価及び監査の段階における手続の実施も容易なものとなる。 （短所） ITを利用した内部統制には短所もある。例えば、その後のシステムの変更の段階で必要な内部統制が組み込まれず、また、プログラムに不正な改ざんや不正なアクセスが行われるなど、全般統制が有効に機能しない場合には、適切な内部統制（業務処理統制）を組み込んだとしても、その有効性が保証されなくなる可能性がある。	御意見いただきありがとうございます。御意見を踏まえ、次のとおり修正させていただきます。 第２章１(2)④ 見出し部分「④ITを利用した内部統制の長所と短所」を「④ITを利用した内部統制の特徴と長所・短所」に修正。 第一段落「ITを利用した内部統制の特徴としては、」を冒頭に記載。また、この修正に伴いその後の文章も所要の修正を実施。 第二段落「統制活動が自動化されている場合」を「その長所としては」に修正。 第三段落「ITを利用した内部統制には短所もある。例えば」を「一方、その短所としては」に修正。
10	付録１の３（２）自動化されたIT業務処理統制の過年度結果の利用について 2007年時点で本件はすでに実施基準および本追補版に記載があった。その際、外部監査人との協議では、表の条件の”変更されていない”という部分に関して、次のようなことを条件としていた。 (1)スクラッチの場合、多くのプログラム変更があるシステムについては、機械的にプログラムの変更管理ができ、短時間で変更がないことが外部監査人も確認できることが適用に必要 (2)IT全般統制で完全に変更がない場合、または、変更が少なく容易にIT業務処理統制に関連する変更がないことを把握できる そして、上記の条件のもと、”周期などは定めず”過年度結果の利用は可能であるということであった パッケージをそのまま利用する場合はパッケージのバージョン、変更点の通知、また、カスタマイズやアドオンについては上記に沿って過年度結果の利用を行っていた。 その後の2011年の実施基準の変更では、手の業務処理統制に複数会計年度に1回のテストでよいことが盛り込まれた。時系列的に考えて、IT業務処理統制の過年度結果の利用のほうが早くから記載されていたので、あとから追加された手の業務処理統制の複数年に1回のテストでよい、という記載が、前のIT業務処理統制の過年度結果の利用の上書きであるという明確な説明は2011年改訂では公には行われなかったように記憶している。しかし、監査人によっては上書きで、過年度結果の利用はせいぜいが2年で3年に1回は実際にテスト、ということになっているようだ。それであれば追補版の記載もそのように変更すべきではないか（小生は実は上書きではなく、（１）（２）のようなところまで厳密にプログラムの変更がないことを証明できれば過年度結果の利用は年限を定めず実施してよいと考えるが）	御意見いただきありがとうございます。付録図表1－2は、数年に一度テストを求めているものとして作成したものではありませんので、原案のとおりとさせていただきます。
11	５０ページのコラム”IT業務処理統制” IT業務処理のテスト内容について、このコラムではITの開発時の”ユーザー受入テスト”レベルのユーザーが業務的に判断できるレベルのテストを想定しているように見える。しかし一方では2007年の導入時点では、システムテストレベルを行うよう求めた監査人もいたようである。ぜひともIT業務処理統制のテストがどちらを想定しているのか明確にしていただけるとありがたい	御意見いただきありがとうございます。このコラムは、IT業務処理統制についての説明であり、ユーザ受入テストやシステムレベルテストの説明を行っているものではありませんので、原案のとおりとさせていただきます。 なお、テストについては、本追補版の他の項目（第４章20ページなど）に記載していますので、御参照のほどよろしくお願いします。
12	システム管理基準（ガイド含む）、情報セキュリティ管理基準との対比について 企業のIT部門にとってはベストプラクティスとして参照することが多いと思われるので、実施基準で求める、特にIT全般統制が何かを理解し、ITに詳しくない会計士の外部監査人がいた場合のコミュニケーションがより円滑になる。日本公認会計士協会の報告もあったほうが良いと思われるが、これは変更が多いので難しいというころがあるのかとは思う。	御意見いただきありがとうございます。本追補版は、実施基準とシステム管理基準等との関係を説明することを目的として策定したものです。いただいた御意見につきましては、システム管理基準追補版の普及のための参考とさせていただきます。