COBIT™

コントロール目標

1998年4月
第2版

COBIT運営委員会および
情報システムコントロール財団

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

目　次

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

ISBN 0-9629440-4-1 (コントロール目標)
ISBN 0-9629440-3-3 (CD-ROM 付き 5 分冊)

印刷：アメリカ合衆国

コントロール目標の原理

＂コントロール目標＂のこの最新版で具体化されたように，COBITは，情報システムの監査とコントロールの専門的職業を維持するのに必要とされる体系的知識（コモン・ボディ・オブ・ノレッジ）を反映している。COBITフレームワークのプロセス毎の高いレベルのコントロールについて焦点をあてているが，コントロール目標はITプロセスに関連する具体的，詳細なコントロール目標に焦点をあてている。フレームワークの34のITプロセスのそれぞれについて３つから30の詳細なコントロール目標がある。コントロール目標は，全般的なフレームワークをITに関する事実上および法律上の国際標準と規則から構成する36の主要な原典からの詳細なコントロール目標と提携させる。それは，IT活動の内において具体的なコントロール手続を実施することによって達成される望ましい結果や目的の表明を含み，それによって，世界中の業界にわたるITコントロールの明確な方針と良い慣行を提供する。

＂コントロール目標＂は，情報サービス，コントロール，監査機能のマネジメントとスタッフに，そして最も重要なビジネス・オーナーに向けられたものである。＂コントロール目標＂はこれらの個人の実用的な小型の文書を提供する。資源利用の有効性，効率性，経済性を保証する正確で明確な最少の定義が明らかにされる。各プロセスについて，詳細なコントロール目標が最低限必要なものとして識別される。つまり，それらのコントロールはコントロール専門家にとって十分性を評価されるものである。本書では，ドメイン／プロセス／コントロール目標関係の概要について述べた302の詳細なコントロール目標が提供されている。コントロール目標によって，フレームワークで説明した概念をITプロセスに適用可能な，具体的なコントロールに言いかえられる。

ドメイン，プロセス，コントロール目標一覧

計画と組織

1.0 戦略的なIT計画の定義

- 1.1 組織の長期および短期計画の一部としてのIT
- 1.2 ITの長期計画
- 1.3 ITの長期計画の策定－方法論と構造
- 1.4 ITの長期計画の変更
- 1.5 情報サービス機能の短期計画の策定
- 1.6 現行システムの評価

2.0 情報基盤の定義

- 2.1情報基盤モデル
- 2.2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
- 2.3 データ分類スキーム
- 2.4 セキュリティレベル

3.0 技術指針の決定

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

4.0 IT組織と関連の定義

- 4.1 情報サービス機能の計画策定あるいは運営委員会
- 4.2 情報サービス機能の組織的な配置
- 4.3 組織的達成のレビュー
- 4.4 役割と責任
- 4.5 品質保証の責任
- 4.6 論理的および物理的セキュリティの責任
- 4.7 オーナシップとカスタディアンシップ
- 4.8 データとシステムのオーナーシップ
- 4.9 監督
- 4.10 職務の分離
- 4.11 IT要員の配員
- 4.12 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
- 4.13 重要なIT要員
- 4.14 契約要員の手続
- 4.15 諸関連

5.0 IT投資の管理

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

6.0 マネジメント目標と指針の伝達

- 6.1 積極的な情報のコントロール環境
- 6.2 方針に対する経営者の責任
- 6.3 組織方針の伝達
- 6.4 方針実施の資源
- 6.5 方針の保守

取得と実施

1.0 解決法の識別

- 1.1 情報要件の定義
- 1.2 代替行動の定式化
- 1.3 取得戦略の立案
- 1.4 第三者機関のサービスの要件
- 1.5 技術的実行可能性の検討
- 1.6 経済的実行可能性の検討
- 1.7 情報アーキテクチャ
- 1.8 リスク分析報告書
- 1.9 コスト効果のあるセキュリティ・コントロール
- 1.10 監査証跡の設計
- 1.11 人間工学
- 1.12 システム・ソフトウェアの選択
- 1.13 調達のコントロール
- 1.14 ソフトウェア製品の取得
- 1.15 第三者機関のソフトウェアの保守
- 1.16 アプリケーション・プログラミングの契約
- 1.17 ファシリティの受理
- 1.18 技術の受理

2.0 アプリケーションソフトウェアの取得と保守

- 2.1 設計方法
- 2.2 既存システムに対する大幅な変更
- 2.3 設計の承認
- 2.4 ファイルの要件定義と文書化
- 2.5 プログラム仕様
- 2.6 原始データの収集設計
- 2.7 入力の要件定義と文書化
- 2.8 インタフェースの定義
- 2.9 ユーザ・マシン・インターフェイス
- 2.10 処理の要件定義と文書化
- 2.11 出力の要件定義と文書化
- 2.12 管理可能性
- 2.13 重要な設計要素としての可用性
- 2.14 アプリケーション・プログラム・ソフトウェアにおけるITのインテグリティ条項
- 2.15 アプリケーション・ソフトウェアのテスト
- 2.16 ユーザの参照資料と支援資料
- 2.17 システム設計の再評価

3.0 技術基盤の取得と保守

- 3.1 新しいハードウェアとソフトウェアの評価
- 3.2 ハードウェアに関する予防保全
- 3.3 システム・ソフトウェアのセキュリティ
- 3.4 システム・ソフトウェアの導入
- 3.5 システム・ソフトウェアの保守
- 3.6 システム・ソフトウェアの変更管理

4.0 ITシステム関連手続の作成と保守

- 4.1 将来の運用要件とサービス水準
- 4.2 ユーザ手続マニュアル

12.2 目立たないITサイト
12.3 訪問者への付添
12.4 要員の健康と安全
12.5 環境要因に対する保護
12.6 無停電電源装置

13.0 運用管理

13.1 処理運用手続と教育マニュアル
13.2 開始プロセスと他の運用文書
13.3 ジョブ･スケジューリング
13.4 標準ジョブ･スケジュールとの差異
13.5 処理の継続
13.6 運用ログ
13.7 遠隔運用

モニタリング

1.0 プロセスのモニタリング

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

2.0 内部統制の妥当性の評価

2.1 内部統制のモニタリング
2.2 内部統制の適時な運用
2.3 内部統制レベルの記録
2.4 運用セキュリティと内部統制の保証

3.0 独立した保証の確保

3.1 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
3.2 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および内部統制の認証／認定
3.3 ITサービスについての独立の有効性評価
3.4 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
3.5 法律と規則の要件と契約上の誓約の独立の準拠性保証
3.6 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
3.7 独立的保証機能の能力
3.8 積極的な監査の関与

4.0 独立的監査の提供

4.1 監査規程
4.2 独立性
4.3 専門家としての倫理と基準
4.4 能力
4.5 計画
4.6 監査業務の実施
4.7 報告
4.8 フォローアップ活動

コントロール目標

次ページ以降は，IT機能の中の34のプロセスの
コントロール目標を詳述したものである。

左のページには，COBITの成果物全体の
整合性を保ち，かつ，理解を容易にするために
***フレームワーク**と同じ高いレベルの*
コントロール目標が記述されている。
ドメインの略称（"ＰＯ"：計画と組織，"ＡＩ"：取得と実施，
"ＤＳ"：デリバリとサポート，"Ｍ"：モニタリング）は
右最上部に表示されている。その次にプロセスの説明があり，
第一次，第二次の重要性の標識も表示されている。
*さらに，**フレームワーク**の説明がリストされ，*
そこで使用されるIT資源がダイアグラムで表示されている。

右ページには，時には2ページ以上にわたることもあるが，
そこのプロセスに適切なコントロール目標が詳述されている。
右ページと左ページの調整のため，ブランクのページが
入ることもある。詳細なコントロール目標は
34のそれぞれのプロセスで展開されている。

PO1

1 戦略的なIT計画の定義

1.1 組織の長期および短期計画の一部としてのIT

コントロール目標

上級経営者は，組織の使命と目標を達成する長期および短期計画を策定し，導入する責任がある。この点において，上級経営者は，諸機会と同様にITの問題が適切に評価され，組織の長期および短期計画に反映されていることを保証すること。

1.2 ITの長期計画

コントロール目標

情報サービス機能の管理者は，組織の全般的な使命と目標の達成を支援するITの長期計画を定期的に策定する責任がある。それ故に，管理者は長期計画の策定プロセスを導入し，構造化された方法論を採用し，標準の計画構造を確立すること。

1.3 ITの長期計画の策定ー方法論と構造

コントロール目標

情報サービス機能の管理者は，長期計画策定のプロセスに関する構造化された方法論を確立し，適用すること。これによって，何を，誰が，いかに，いつ，そして，なぜ，という基本的な質問を網羅する高品質の計画をもたらすであろう。計画策定のプロセスで考慮され，適切に問題提起される側面は，その組織モデルとその変化，地理的分布状況，技術的発展，コスト，法律と規制の要件，第三者機関あるいは市場の要件，計画の範囲，ビジネスプロセスリエンジニアリング，配員，イン／アウトソーシングなどである。それらの選択でもたらされる便益は，明確に識別されること。計画自体は，組織の品質計画と情報リスク管理計画のような他の計画についても言及すること。

1.4 ITの長期計画の変更

コントロール目標

情報サービス機能の管理者は，組織の長期計画の変更，IT状況の変化に適応するためにITの長期計画を適時に，正確に修正する適切なプロセスがあることを保証すること。

1.5 情報サービス機能の短期計画の策定

コントロール目標

情報サービス機能の管理者は，ITの長期計画がITの短期計画に定期的に反映されていることを保証すること。そのような短期計画は，適切なITサービス部門の資源が，ITの長期計画と整合性のある基礎のもとで配分されていることを保証すること。短期計画は，ビジネスとITの状況変化に応じて，定期的に再評価され，必要に応じて修正されること。フィージビリティスタディの適時な実行は，短期計画の実施が適切に開始されることを保証すること。

1.6 現行システムの評価

コントロール目標

情報サービス機能の管理者は，戦略的なIT計画の開発または変更に先立って，現行システムが組織のビジネス要件をどの程度サポートしているかを判定する目的で，現行システムについて，ビジネスの自動化の程度，機能性，安定性，複雑性，コスト，強みと弱みの点から評価すること。

PO2

2 情報基盤の定義

2.1 情報基盤モデル

コントロール目標

情報は，必要性と整合性が保たれ，人々が効果的に適時に責任を果たすことが出来るような形態と時間枠で識別され，捕捉され，伝達されること。それゆえに，情報サービス機能は，コーポレート･データ･モデルと関連した情報システムを包含する情報アーキテクチャモデルを創り，定期的に更新すること。情報アーキテクチャ･モデルは，ITの長期計画と整合性が保たれていること。

2.2 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

コントロール目標

情報サービス機能は，組織のデータ･シンタックス･ルールを組み入れたコーポレート･データ･ディクショナリを作成し，継続して更新することを保証すること。

2.3 データ分類スキーム

コントロール目標

全般的な分類のフレームワークは，情報クラス（つまり，セキュリティ分類）へのデータの位置付けに関連して，オーナーシップの割当と同様確立されること。クラスに対するアクセス規約が適切に定義されること。

2.4 セキュリティレベル

コントロール目標

管理者は，「保護の必要がない」というレベルから，上記で識別されたデータ分類の各々についてのセキュリティレベルを定義し，導入し，維持すること。これらのセキュリティレベルは，各々の分類についての適切な（最小）セキュリティとコントロール対策を表していること。

PO3

3 技術指針の決定

3.1 技術基盤の計画策定

コントロール目標

情報サービス機能は，ITの長期および短期計画に従って技術基盤計画を策定し，定期的に更新すること。そのような計画は，システム基盤，技術指針，移行戦略のような側面を含むこと。

3.2 将来の動向と規制のモニタリング

コントロール目標

将来の動向と規制状況に関する継続的なモニタリングは，技術基盤計画を策定し，維持する間，これらの要素が考慮できるように，情報サービス機能によって確保されること。

3.3 技術基盤のコンティンジェンシー

コントロール目標

技術基盤計画は，不測事態の側面（つまり，基盤の冗長性，変化からの回復力，適切性と展開能力）が体系的に評価されること。

3.4 ハードウェアとソフトウェアの取得計画

コントロール目標

情報サービス機能の管理者は，ハードウェアとソフトウェアの取得計画が策定され，技術基盤計画において識別されたニーズを反映していることを保証すること。

3.5 技術標準

コントロール目標

技術基盤計画に基づいて，管理者は標準化を促進するために技術的な平均水準を定義すること。

PO4

4 IT組織と関連の定義

4.1 情報サービス機能の計画策定あるいは運営委員会

コントロール目標

組織の上級管理者は，情報サービス機能とその活動を監視するために，計画または運営委員会を設置すること。委員会メンバーには，経営者，ユーザ部門の管理者と情報サービス機能からの代表者を含むこと。委員会は，定期的に会合を開催し，経営者に報告すること。

4.2 情報サービス機能の組織的な配置

コントロール目標

全般的な組織構造に情報サービス機能を配置する際，上級管理者は，有効なITの解決策と解決策を実施する際，十分な進展があることを保証し，さらに，ITの課題を識別し，解決する際の意識，理解，技能を増進するのを支援するため，最高経営者とのパートナーシップを築くために必要なほど，権威と，要員数と，ユーザ部門から独立していることを保証すること。

4.3 組織的達成のレビュー

コントロール目標

継続して，目標と変貌する環境を満たすために，組織的構造をレビューする適切なフレームワークがなければならない。

4.4 役割と責任

コントロール目標

管理者は，組織全員が情報システムに関連して役割と責任をもち，かつそれを知っていることを保証すること。全員が自身に与えられた役割と責任を行使するための，十分な権限をもつこと。誰もが内部統制とセキュリティに対する責任をある程度もっているという意識付けがされること。従って，定期的な運動が意識喚起と規律を増進するために組織化され，実施されること。

4.5 品質保証の責任

コントロール目標

管理者は，情報サービス機能のスタッフメンバに品質保証機能の活動責任を割当て，情報サービス機能の品質保証グループに適切な品質保証，システム，コントロール，コミュニケーションの専門的知識があるを確保すること。情報サービス機能に組織的配置することで，品質保証グループの責任と規模は，組織の要件を満たすこと。

4.6 論理的および物理的セキュリティの責任

コントロール目標

管理者は，組織の上級管理者に直属する情報セキュリティ管理者に組織の情報資産の論理的かつ物理的セキュリティの双方を保証する責任を正式に割当てること。最低限，セキュリティ管理者の責任は，組織における全般的なセキュリティの課題に対処するために，組織全体にわたる階層で確立されること。必要ならば，追加のセキュリティ管理者の責任は，関連したセキュリティ問題を解決するために，システム固有のレベルで割当てられること。

4.7 オーナーシップとカスタディアンシップ

コントロール目標

管理者は，正式にデータのオーナとカスタディアンを任命する仕組みを作ること。彼らの役割と責任は，明確に定義されること。

4.8 データとシステムのオーナーシップ

コントロール目標

管理者は，全ての情報資産（データとシステム）が，分類とアクセス権限について決定する任命されたオーナを有することを確保すること。システムのオーナは，典型的には，システムのデリバリ／運用グループに対して，日常のカスタディアンシップをセキュリティ管理者にセキュリティ責任を任せる。オーナは，しかし，適切なセキュリティ対策の維持については責任が残る。

4.9 監督

コントロール目標

上級管理者は，役割と責任が適切に行使され，要員全てがその役割と責任を果たすのに十分な権限と資源をもっているかどうかを評価し，重要業績指標を全般的にレビューすることを保証するために，情報サービスの組織において適切な監督実務を行うこと。

4.10 職務の分離

コントロール目標

上級管理者は，一個人が重要なプロセスを滅ぼす可能性を除外する役割と責任の分離を図ること。管理者は，要員が自らの個々の業務と職位について定められた職務のみを果たしていることを確認することも必要である。特に，以下の職務の分離が維持されること。

- －情報システムの利用
- －データの入力
- －コンピュータの運用
- －ネットワークの管理
- －システムの管理
- －システムの開発と保守
- －変更の管理
- －セキュリティの管理，および，
- －セキュリティの監査

4.11 IT要員の配置

コントロール目標

情報サービス機能が十分な数の能力のあるITスタッフを有することを保証するために，配員の要件評価は，定期的に実施されること。配員の要件は，少なくとも年次またはビジネス業務やITの環境に大幅な変化が生じた場合，評価されること。評価結果は，適切な現在および将来における要員を確保するために迅速に行動に生かされること。

4.12 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

コントロール目標

管理者は，情報サービス機能のスタッフに関する職位記述書が作成され，定期的に更新されることを保証すること。これらの職位記述書は，権限と責任について明確に詳しく述べ，関連する職位で必要とされる能力と経験の定義を含み，業績評価の利用に適していることも保証されること。

4.13 重要なIT要員

コントロール目標

管理者は，重要なIT要員を定義し，識別すること。

4.14 契約要員の手続

コントロール目標

管理者は，組織の情報資産の保護を確保するために，情報サービス機能にるコンサルタントおよび他の契約要員の活動を統制する関連手続を定義し，実施すること。

4.15 諸関連

コントロール目標

情報サービス機能の管理者は，情報サービス機能と多様なその他の情報サービス機能の内部および外部（つまり，ユーザ，供給者，セキュリティオフィサ，リスクマネジャ）の利害関係者間の最適な調整，伝達，連絡の構造を確立し，維持するのに必要な行動をとること。

PO5

5 IT投資の管理

5.1 情報サービス機能の年次運営予算

コントロール目標

上級管理者は，年次の情報サービス機能の運営予算がITの長期および短期計画とともに，組織の長期および短期の計画と整合して作成され，承認されることを保証する予算策定プロセスを履行すること。代替的な資金調達が調査されること。

5.2 コストと便益のモニタリング

コントロール目標

管理者は，実績と予算を比較するコストモニタリングププロセスを確立すること。さらに，ITの活動から得ることができる便益が，測定され，報告されること。コストのモニタリングのためには，実績値の出所は，組織の会計システムに基づく必要があり，そのシステムは，情報サービス機能活動に関連するコストを定期的に記録，処理し，報告すること。便益のモニタリングのためには，高次のパフォーマンス指標が決定され，適切性に対して定期的に，報告され，レビューされること。

5.3 コストと便益の正当化

コントロール目標

マネジメントコントロールは，情報サービス機能によるサービスのデリバリが，コスト面から正当化され，業界水準に整合していることを適切に保証すること。ITの活動から得られることができる便益は，同様に分析されること。

PO6

6 マネジメント目標と指針の伝達

6.1 積極的な情報のコントロール環境

コントロール目標

管理者は，人間の誠実さ，倫理価値観および能力，管理者の哲学と業務のスタイル，取締役会によって提供される会計責任，注意および指示のような側面を検討することによって，組織全体を通じて，積極的なコントロール環境を醸成するフレームワークと意識喚起プログラムを創ること。特定の注意がITの側面に対し払われること。

6.2 方針に対する経営者の責任

コントロール目標

管理者は，全般的な目的と指示を網羅する方針の公式化，作成，文書化，公表とコントロールに完全な責任を負う。方針の適切性に関する定期的なレビューが実行されること。成文化された方針と手続の複雑性は，組織規模と管理スタイルに常に整合していること。

6.3 組織方針の伝達

コントロール目標

管理者は，組織的方針が組織の全階層に伝達され，理解されることを確保すること。

6.4 方針実施の資源

コントロール目標

伝達の後で，方針の実施に適切な資源を管理者によって取っておくこと。管理者は，また，方針の実施の適時性をモニタリングすること。

6.5 方針の保守

コントロール目標

方針は，変化する状況に順応するよう定期的に調節されること。方針は，それらの十分性と適切性を評価するために，少なくとも年次または業績あるいはビジネス環境への顕著な変化に基づいて再評価され，必要に応じて修正されること。管理者は，定期的なレビューおよび基準，方針，指示，手続の承認についてのフレームワークおよびプロセスを提供すること。

6.6 方針，手続および標準への準拠

コントロール目標

管理者は，要員が導入された方針と手続を理解し，方針と手続が遵守されつつあるかどうかを確かめるために，適切な手続があることを確認すること。倫理的，セキュリティおよび内部統制基準への準拠性手続が最高経営層によって設けられ，例示によって促進されること。

6.7 品質の協定

コントロール目標

情報サービス機能の管理者は，全社的哲学とこの点に関する哲学と整合性のある品質の哲学，方針と目標を定義し，文書化し，維持すること。品質の哲学，方針，目標は，情報サービス機能の階層全てに理解され，導入され，維持されること。

6.8 セキュリティおよび内部統制フレームワークの方針

コントロール目標

上級管理者は，セキュリティと内部統制に対する組織の全般的な方法論を確立するフレームワークの方

針の作成と維持に全面的な責任を負うこと。方針は，ビジネス目標全体に準拠し，予防対策，異常の適時な識別，損失の制限および適時な復旧によって，リスクを最小化することを目指していること。対策は，費用便益分析に基づき，優先順位がつけられること。さらに，上級管理者は，この高い水準のセキュリティと内部統制の方針が目的と目標，管理構造，組織内の範囲，すべてのレベルにおける実施責任者の定義と任命，およびセキュリティと内部統制の方針に準拠していないことに関連する罰則と懲戒処分を定義していることを確保すること。

6.9 知的財産権

コントロール目標

管理者は，開発ソフトウェアについて，契約と同じく内製をも対象として，知的財産権に関して文書化された方針を提供し，実施すること。

6.10 特定課題の方針

コントロール目標

特定の活動，アプリケーション，システムあるいは技術を検討する際，管理者の決定を文書化するための課題特有の方針が作成されることを保証する適切な基準が設定されること。

6.11 ITセキュリティ意識の伝達

コントロール目標

ITセキュリティ意識の計画は，各々のITユーザにITセキュリティ方針を伝達し，ITセキュリティの重要性について完全に理解されることを保証すること。それはITセキュリティが組織，すべての従業員に便益をもたらし，すべての人々がそれに責任を負っているというメッセージを伝えること。ITセキュリティ意識の計画は，上級管理者の観点から支持され，表現されること。

PO7

7 人的資源の管理

7.1 要員の採用と昇進

コントロール目標

管理者は，要員の募集と昇進の慣行の実務が客観的な規準に基づいており，教育，経験および責任を考慮していることを保証するために必要とされるプロセスを導入し，定期的に評価すること。これらのプロセスは，この点に関する組織の全般的な方針および手続と整合性がなければならない。

7.2 要員の資格

コントロール目標

情報サービス機能の管理者は，特定のタスクを実施する要員は，要求される適切な教育，訓練や経験の上で資格があることを定期的に検証すること。管理者は，専門家組織のメンバーシップを得るよう奨励すること。

7.3 要員の教育

コントロール目標

管理者は，従業員が採用に当たり導入教育を受けていること，知識，技能，能力と効果的に業務を行うのに必要とされる水準までのセキュリティ意識を維持するための継続教育がなされていることを保証すること。要員の技術および管理技能の水準を効果的に上げるために行われる教育と訓練プログラムは，定期的にレビューされること。

7.4 相互教育あるいは代替要員

コントロール目標

管理者は，利用不可能性に対処するために，識別された重要な要員の十分な相互訓練または代替を準備すること。機密情報を扱う職位にある要員は，利用不可能性に対処すること，不正行為を発見する組織能力を行使できる程十分長い期間の中断しない休暇を取るように要求されること。

7.5 要員の身元調査手続

コントロール目標

情報サービス機能の管理者は，その部門の要員が採用され，異動あるいは昇進する前に職位の機密性に基づいて，身元調査手続に従っていることを保証すること。最初に採用されたとき，そのような身元調査手続に従っていなかった従業員は，セキュリティの身元調査手続が取得されるまで，機密の職位についていないことが保証されること。

7.6 従業員の業績評価

コントロール目標

管理者は，従業員の業績評価プロセスを設け，作成された基準と定期的に特定業務の責任に照らして，評価が行われていることを確かめること。従業員は，必要であれば業務あるいは行動についてのカウンセリングを受けること。

7.7 職務の交替および終了

コントロール目標

管理者は，内部統制とセキュリティが業務の交替や業務の終了によって損なわれないように，職務交替変更と職務の終了に関して適切かつ適時な行動がとられていることを保証すること。

PO8

8 外部要件への準拠性の保証

8.1 外部要件のレビュー

コントロール目標

組織は，外部の要件レビューとこれらの諸活動の調整手続を作成し，維持すること。継続的な調査が組織にとって，適用可能な外部要件であるかを判断すること。ITの実務とコントロールに関連する法的，政府または他の外部要件は，レビューされること。管理者は，また，情報サービス機能の戦略が任意の関連する第三者機関の要件を準拠または支援する必要がある範囲の判断を含む，組織の全般的な情報ニーズに対する任意の外部関係の影響を評価すること。

8.2 外部要件に準拠するための実務と手続

コントロール目標

組織の実務は，外部要件との準拠性を保証するために，適時に適切な是正行動が取られていることを保証すること。さらに，継続して遵守されていることを保証する適切な手続は，作成され，維持されること。この点に関して必要であれば，管理者は法務助言を受けること。

8.3 安全と人間工学への準拠

コントロール目標

管理者は，情報サービス機能のユーザと要員の執務環境において，安全と人間工学標準が遵守されていることを保証すること。

8.4 プライバシー，知的財産権とデータフロー

コントロール目標

管理者は，組織のITの実務が適用可能なプライバシー，知的財産権，越境データフローおよび暗号化規制に準拠していることを保証すること。

8.5 電子商取引

コントロール目標

管理者は，通信プロセス，ならびに，取引メッセージセキュリティおよびデータ保管のための基準について，取引パートナー間における合意に関する正式な契約が，適切に作成されていることを保証すること。インターネットを通じて取引が行われる場合には，管理者は，現地法と世界的な慣習に準拠していることを保証する適切なコントロールを実施すること。

8.6 保険契約への準拠

コントロール目標

管理者は，保険契約の要件が適切に識別され，継続して充足されていることを保証すること。

PO9

9 リスク評価

9.1 ビジネスリスクの評価

コントロール目標

管理者は，体系的なリスク評価フレームワークを作成すること。そのようなフレームワークは，どのようにリスクが受容可能なレベルに管理されるべきかを判定する基礎を形成しながら，ビジネスの目標達成に関連する情報リスクの定期的な評価を組み込むこと。プロセスは，全体のレベルおよび特定システムのレベル（繰り返しと，新しいプロジェクトの両方）について，リスク評価を提供する必要があり，また，監査，検査および識別された事象の結果から得られたリスク評価情報の定期的な更新を保証すること。

9.2 リスク評価方法論

コントロール目標

管理者は，範囲と境界，リスク評価に採用される方法論，責任および必要とされる技能を定義する一般的なリスク評価方法論を確立すること。リスク評価の品質は，構造化された方法と熟練したリスク評定者によって保証されること。

9.3 リスクの識別

コントロール目標

リスク評価方法論は，資産，脅威，脆弱性，安全保護，脅威の結果と可能性というような本質的なリスク要素の検討に焦点を当てること。

9.4 リスクの測定

コントロール目標

リスク評価方法論は，リスク識別情報の分析により検討領域が危険に曝されているリスクの定量的または定性的（または結合された）測定値が得られることを保証すること。組織のスク受容能力も，また評価されること。

9.5 リスクの行動計画

コントロール目標

リスク評価方法論は，コスト効果的なコントロールとセキュリティ対策が，継続して，リスクに対するエクスポージャを軽減していることを保証するリスク行動計画の定義を提供すること。

9.6 リスクの受容

コントロール目標

リスク評価方法論は，リスク識別と測定，組織の方針，リスク評価方法論自体に内在する不確実性，安全保護とコントロールを実施するコストと効果に依存して，残余のリスクを正式に受容することを保証すること。残余のリスクは，適切な保険担保で相殺されること。

PO10

10 プロジェクト管理

10.1 プロジェクト管理のフレームワーク

コントロール目標

管理者は，遂行中の各プロジェクトに採用され，適用されるプロジェクト管理方法論と同様，プロジェクトを管理する範囲と境界を定義する全般的なプロジェクト管理フレームワークを確立すること。方法論は，最低限，責任の分担，タスクの分割，時間と資源の予算策定，里程標，チェックポイントおよび承認を網羅すること。

10.2 プロジェクト開始におけるユーザ部門の参画

コントロール目標

組織のプロジェクト管理フレームワークは，開発，実施あるいは改訂プロジェクトの定義および承認において影響を受けるユーザ部門管理者による参画を提供すること。

10.3 プロジェクトチームメンバと責任

コントロール目標

組織のプロジェクト管理フレームワークは，プロジェクトのスタッフメンバの任命基準を明記し，プロジェクトチームメンバの責任と権限を定義すること。

10.4 プロジェクトの定義

コントロール目標

組織のプロジェクト管理フレームワークは，プロジェクト業務を開始する前に，導入プロジェクトの性格と範囲を明確に文書化し，定義する明瞭に記述した文書の作成を提供すること。

10.5 プロジェクトの承認

コントロール目標

組織のプロジェクト管理フレームワークは，各提案されたプロジェクトについて，組織の上級管理者がプロジェクトを進めるかどうかについて決定する基礎として，関連する実行可能性の検討報告書をレビューしていることを保証すること。

10.6 プロジェクトフェーズの承認

コントロール目標

組織のプロジェクト管理フレームワークは，次のフェーズの業務を開始する前に，サイクルの各フェーズで達成された業務を承認するために，ユーザと情報サービス機能の指名された管理者を提供すること。

10.7 プロジェクトマスタ計画

コントロール目標

管理者は，承認された各プロジェクトについて，ライフを通じてのプロジェクトのコントロールを維持するのに適切で，プロジェクトのライフを通じて要した時間とコストをモニタリングする方法を含むプロジェクトマスタ計画を確保すること。

10.8 システムの品質保証計画

コントロール目標

新規または改訂システムの実施がプロジェクトマスター計画に統合され，関係する関係者全てによって正式にレビューおよび合意される品質計画の作成を含んでいることを保証すること。

10.9 保証方法の計画策定

コントロール目標

保証タスクは，プロジェクト管理フレームワークの計画フェーズにおいて識別されなければならない。保証タスクは，新規または改訂システムの認可を支援し，内部統制とセキュリティの点が関連要件を満たしていることを保証すること。

10.10 正式なプロジェクト・リスク管理

コントロール目標

管理者は，個々のプロジェクトに関連したリスクを消去あるいは，最小化する正式なプロジェクト・リスク管理プログラム（つまり，欲っしていない変化を引き起す潜在性のあるものをもつ領域または事象を識別およびコントロールすること）を導入すること。

10.11 テスト計画

コントロール目標

組織のプロジェクト管理フレームワークは，テスト計画が開発，導入，改訂プロジェクトについて作成されていること。

10.12 教育計画

コントロール目標

組織のプロジェクト管理フレームワークは，教育計画が各開発，実施，改訂プロジェクトについて作成されていること。

10.13 導入後レビュー計画

コントロール目標

組織のプロジェクト管理フレームワークは，プロジェクトチーム活動の重要な部分として，プロジェクトが計画された効果をデリバリしていることを確かめるために，新規または改訂の情報システムの導入後レビュー計画の作成を提供すること。

PO11

11 品質管理

11.1 全般的品質計画

コントロール目標

上級管理者は，組織およびITの長期計画に基づいて，全般的な品質計画を作成し，定期的に維持すること。計画は，継続的な改善の哲学を推進し，何を，誰が，どのようにという基本的な質問に答えること。

11.2 品質保証の方法論

コントロール目標

管理者は，全般およびプロジェクトに特定した品質保証活動を網羅する品質保証に関する標準的な方法論を確立すること。方法論は，品質保証活動の種類（レビュー，監査，検査などのような）が全般的な品質計画の目標を達成するのに実施すべく定められること。それはまた，固有の品質保証レビューを要求すること。

11.3 品質保証の計画策定

コントロール目標

管理者は，品質保証活動の範囲と時期を決定するために，品質保証の計画策定プロセスを導入すること。

11.4 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

コントロール目標

管理者は，品質保証の要員に与えられた責任が，情報サービス機能の標準と手続に全般的に準拠しているかのレビューを含むことを保証すること。

11.5 システム開発ライフサイクル方法論

コントロール目標

組織の上級管理者は，情報システムの基準を定義し，導入し，コンピュータ化された情報システムと関連技術の開発，取得，実施および保守プロセスを統制するシステム開発ライフサイクル方法論を採用すること。選定されたシステム開発ライフサイクル方法論は，開発され，取得され，実施され，保守されるシステムにとって適切であること。

11.6 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

コントロール目標

既存技術に大幅な変更が生じた場合，管理者は，新しい技術の取得の場合と同様に，システム開発ライフサイクル方法論を遵守しなければならない。

11.7 システム開発ライフサイクル方法論の更新

コントロール目標

上級管理者は，システム開発ライフサイクル方法論の条項が現在の一般に認められた技術と手続を反映していることを保証するために，定期的なレビューを導入すること。

11.8 調整と伝達

コントロール目標

管理者は，情報サービス機能のカスタマとシステム実施者の間で，緊密な調整と伝達を保証するプロセスを確立すること。このプロセスは，ビジネス要求を満たす上質なITソリューションの条項を保証するシステム開発ライフサイクル方法論を用いて構造化された方法論として必然的に伴うこと。管理者は，システム

開発ライフサイクルを通じて，緊密な協力と伝達によって特徴づけられる組織を推進すること。

11.9 技術基盤に関する取得と維持のフレームワーク

コントロール目標

技術基盤の取得と維持に関して，一般的なフレームワークが適切であること。技術基盤にして従うべき異なった手順（取得，プログラミング，文書化とテスト，パラメータ設定，保守と修正の適用のような）は，技術基盤のフレームワークの取得と維持によって統制され，整合性が取れていること。

11.10 第三者機関による実施者の関係

コントロール目標

管理者は，第三者機関の導入者との良好な基礎的関係を保証するプロセスを導入すること。そのようなプロセスは，ユーザと導入者が検収基準，変更の処理，開発中の諸問題，ユーザの役割，ファシリティ，ツール，ソフトウェア，基準および手続についての一致を提供すること。

11.11 プログラムの文書化標準

コントロール目標

組織のシステム開発ライフサイクル方法論は，関係スタッフに伝達され，強制されるプログラム文書化基準を組み込むこと。方法論は，情報システムの開発または改訂プロジェクトで作成されたドキュメンテーションが，これらの諸基準に一致していることを保証すること。

11.12 プログラムテスト標準

コントロール目標

組織のシステム開発ライフサイクル方法論は，個々のソフトウェアの単体と結合プログラムのテストのためのテスト要件，検証，文書化および維持を情報システムの開発または改訂プロジェクトの一部として作成された導入の維持を網羅する標準を提供すること。

11.13 システムテスト標準

コントロール目標

組織のシステム開発ライフサイクル方法論は，システム全体のテストのテスト要件，検証，文書化および維持を情報システム開発または改訂プロジェクトの一部として網羅する標準を提供すること。

11.14 並行／パイロットテスト

コントロール目標

組織のシステム開発ライフサイクル方法論は，新規や既存システムが実行されるであろうところの並行またはパイロットテスト環境を定義すること。

11.15 システムテストの文書化

コントロール目標

組織のシステム開発ライフサイクル方法論は，すべての情報システムの開発，実施または改訂プロジェクトの一部として，システムテストの文書化された結果を保存すること。

11.16 開発標準に対する準拠性の品質保証評価

コントロール目標

組織の品質保証の方法論は，運用中の情報システムの導入後レビューが，プロジェクトチームがシステム開発ライフサイクル方法論の条項に従っているかどうかを評価することを要求すること。

11.17 情報サービス機能の目標達成の品質保証レビュー

コントロール目標

品質保証の方法論は，特定システムとアプリケーション開発活動が情報サービス機能の目標を達成した程度のレビューを含むこと。

11.18 品質測定基準

コントロール目標

管理者は，たとえば，品質目標が達成されたか否かを評価するように，活動の結果を測定する測定基準を決定し使用すること。

11.19 品質保証レビューの報告書

コントロール目標

品質保証レビューの報告書が作成され，ユーザ部門と情報サービス機能の管理者に提出されること。

AI1

1 解決法の識別

1.1 情報要件の定義

コントロール目標

組織のシステム開発ライフサイクル方法論は，現行システムによって満たされ，また，提案された新しい，または改訂システム（ソフトウェア，データおよび基盤）によって満たされる予定のビジネス要件が，開発，実施または改訂プロジェクトが承認される前に，明確に定義されることを規定すること。システム開発ライフサイクル方法論は，解決策の機能的および運用への要件が，性能，安全，信頼性，互換性，セキュリティおよび規制を含め明記されることを要求すること。

1.2 代替行動の定式化

コントロール目標

組織のシステム開発ライフサイクル方法論は，提案された新しいまたは改訂システムのために確立されたビジネス要件を満たすであろう代替行動の分析を規定すること。

1.3 取得戦略の立案

コントロール目標

組織のシステム開発ライフサイクル方法論は，ソフトウェアの取得が，パッケージ，内製，契約または既存ソフトウェアの強化，あるいは，これらすべての組み合わせ，で行われるのかを決定するソフトウェア取得戦略計画を提供すること。

1.4 第三者機関のサービスの要件

コントロール目標

組織のシステム開発ライフサイクル方法論は，第三者機関のサービス・ベンダと取引する際のRFP（提案要求書）の要件と仕様の評価方法を提供すること。

1.5 技術的実行可能性の検討

コントロール目標

組織のシステム開発ライフサイクル方法論は，提案された新しいまたは改訂の情報システムプロジェクトのために確立されたビジネス要件を満たす各代替案の技術的な実行可能性の検討を規定すること。

1.6 経済的実行可能性の検討

コントロール目標

組織のシステム開発ライフサイクル方法論は，提案された情報システムの開発，導入，改訂プロジェクトにおいて確立されたビジネス要件を満たすために考えられつつある各代替案に関連する費用対効果の分析を提供すること。

1.7 情報アーキテクチャ

コントロール目標

管理者は，解決策が識別され，また，実行可能性が分析されつつある間，企業データ・モデルに注意が払われていることを保証すること。

1.8 リスク分析報告書

コントロール目標

組織のシステム開発ライフサイクル方法論は，各提案された情報システム開発，実施，または改訂プロジェクトにおいて，セキュリティの脅威の分析と文書化，潜在的な脆弱性と影響，識別されたリスクを減少さ

せ，または消滅させる実行可能なセキュリティと内部統制の安全保護を提供すること。これは全般的なリスク評価のフレームワークと整合性をとって実現されること。

1.9 コスト効果のあるセキュリティ･コントロール

コントロール目標

管理者は，コントロールの費用が効果を超えないことを保証するために，セキュリティの費用と効果が注意深く貨幣および非貨幣単位で検討されていることを保証すること。決定は正式な管理者の署名を必要とする。

1.10 監査証跡の設計

コントロール目標

組織のシステム開発ライフサイクル方法論は，監査証跡についての適切な機構が利用可能であり，または識別され，選択された解決策のために開発できることを要求すること。その機構は，開示や悪用から，センシティブデータを保護する能力（例，ユーザID）を提供すること。

1.11 人間工学

コントロール目標

管理者は，情報サービス機能によって実施される情報システムの開発，実施および改訂プロジェクトが，自動化解決策の導入に関連する人間工学的な課題に注意を払っていることを保証すること。

1.12 システム･ソフトウェアの選択

コントロール目標

管理者は，運用要件を満たす全ての潜在的システム･ソフトウェア･プログラムを識別するために，情報サービス機能によって標準的手続が遵守されていることを保証すること。

1.13 調達のコントロール

コントロール目標

管理者は，IT関連のハードウェア，ソフトウェアおよびサービスの調達において遵守しなければならない共通の手続と基準を記述する全社的なの調達方法論を作成し，導入すること。製品は，使用と財務決済に先立ってレビューされ，テストされること。

1.14 ソフトウェア製品の取得

コントロール目標

ソフトウェア製品の取得は，組織の調達方針を遵守すること。

1.15 第三者機関のソフトウェアの保守

コントロール目標

管理者は，第三者機関のプロバイダから得たライセンスされたソフトウェアについて，プロバイダがソフトウェア製品のインテグリティ権利を検証し，保護し，維持する適切な手続をもっていることを要求すること。出荷された製品に関連する保守契約書にある製品の支援に考慮すること。

1.16 アプリケーション･プログラミングの契約

コントロール目標

組織のシステム開発ライフサイクル方法論は，契約プログラミング･サービスの調達が，情報サービス機能の任命されたメンバーからの書面によるサービスの要請によって正当化されることを示すこと。契約書は，ソフトウェア，ドキュメンテーションおよび他の成果物が検収に先だってテストされ，レビューされていることを明記すること。さらに，完了した契約プログラミング･サービスの最終製品が仕事の支払，最終製品の承認前に，情報サービス機能の品質保証グループその他の関係者（ユーザ，プロジェクト管理者など）

によって関連基準に従ってテストされ，レビューされていることを要求すること。契約の仕様に含まれるべきテストには，システムテスト，統合テスト，ハードウェアと要素テスト，手続テスト，負荷および強度テスト，調整と性能テスト，復帰テスト，ユーザ検収テスト，そして最後に予想しないシステムの不具合を回避するために全システムのパイロットテストにより構成されること。

1.17 ファシリティの受理

コントロール目標

管理者は，提供されるファシリティの検収計画は，契約書において供給者と合意され，この計画が検収手続と規準を定義していることを確保すること。さらに，契約書で明示された要件を満たす設備と環境を保証するために，検収テストが実施されること。

1.18 技術の受理

コントロール目標

管理者は，提供される特定の技術が提供出来る検収計画は，契約書において供給者と合意され，この計画が検収手続と規準を定義していることを確保すること。さらに，計画で規定された検収テストには，検査，機能テストおよび負荷テストを含むこと。

AI2

2 アプリケーションソフトウェアの取得と保守

2.1 設計方法

コントロール目標

組織のシステム開発ライフサイクル方法論は，緊密なシステムユーザとの連絡を含む適切な手続と技術が，各新情報システム開発プロジェクトに関する設計仕様を作成し，ユーザ要件に対して設計仕様を検証するために適用されていることを提供すること。

2.2 既存システムに対する大幅な変更

コントロール目標

管理者は，既存システムに大幅な変更が起こった場合，新しいシステムの開発と同様の開発プロセスが遵守されていることを確保すること。

2.3 設計の承認

コントロール目標

組織のシステム開発ライフサイクル方法論は，全ての情報システム開発と改訂プロジェクトの設計仕様が，必要であれば，管理者，影響を受けるユーザ部門および組織の上級管理者によってレビューされ，承認されることを要求すること。

2.4 ファイルの要件定義と文書化

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システムの開発または改訂プロジェクトについてのファイルフォーマットの定義および文書化に適切な手続が適用されることを提供すること。このような手続は，データディクショナリ規約が尊重されていることを保証すること。

2.5 プログラム仕様

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システムの開発または改訂プロジェクトについて詳細な文書化されたプログラム仕様書が作成されることを要求すること。方法論は，さらにプログラム仕様がシステム設計仕様に合致していることを保証すること。

2.6 原始データの収集設計

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システムの開発または改訂プロジェクトについて，データの収集および入力の適切な仕組みが明記されることを要求すること。

2.7 入力の要件定義と文書化

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システム開発または改訂プロジェクトについて，入力要件を定義し，文書化する適切な仕組みが存在することを要求すること。

2.8 インタフェースの定義

コントロール目標

組織のシステム開発ライフサイクル方法論は，すべての外部および内部のインタフェースが適切に，仕様化され，設計され，そして，文書化されることを提供すること。

2.9 ユーザ･マシン･インタフェース

コントロール目標

組織のシステム開発ライフサイクル方法論は，使い易くそして自動文書化（オンラインヘルプ機能によって）できる，ユーザとマシン間のインタフェースの開発を提供すること。

2.10 処理の要件定義と文書化

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システム開発または改訂プロジェクトについて，処理要件を定義し，文書化する適切な仕組みが存在することを要求すること。

2.11 出力の要件定義と文書化

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システム開発または改訂プロジェクトについて，出力要件を定義し，文書化する適切な仕組みが存在することを要求すること。

2.12 管理可能性

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システムの開発または改訂プロジェクトについて，内部統制およびセキュリティ要件が仕様されていることを保証する適切な仕組みを要求すること。方法論は，さらに，入力，処理，出力の正確性，完全性，適時性および承認を保証するアプリケーション･コントロールを含むように，情報システムが設計されることを保証すること。機密性評価は，システムの開発あるいは改訂の開始において，実行されること。開発あるい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統合するために，システムの概念設計に沿って評価されること。

2.13 重要な設計要素としての可用性

コントロール目標

組織のシステム開発ライフサイクル方法論は，できるだけ早い段階で，新しいまたは改訂情報システムの設計プロセスで可用性が考慮されること。可用性は分析され，必要ならば，保守性と信頼性の向上を通じて増進されること。

2.14 アプリケーション･プログラム･ソフトウェアにおけるITのインテグリティ条項

コントロール目標

組織は適用できるならば，アプリケーション･プログラムがロールバック等の方法によりインテグリティを回復することでデータインテグリティを確保することを支持するために，ソフトウェアによって実行される業務を定常的に検証する条項を含むことを保証する手続を作成すること。

2.15 アプリケーション･ソフトウェアのテスト

コントロール目標

アプリケーション･ソフトウェアがユーザによって承認される前に，ユニットテスト，アプリケーションテスト，統合テスト，システムテストと負荷および強度テストをプロジェクトテスト計画および確立したテスト基準に従って実施されること。テスト中，使用する機密情報の開示を防止するために適切な対策を実施すべきである。

2.16 ユーザの参照資料と支援資料

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システムの開発または改訂プロジェクトの一部として，適切なユーザ･レファレンスとサポート･マニュアル（電子的フォーマットが望ましい）が作成されるこ

と。

2.17 システム設計の再評価

コントロール目標

組織のシステム開発ライフサイクル方法論は，システム開発または保守の最中で著しい技術的／論理的な齟齬が発生した場合はいつでも，システム設計は再評価されることを保証すること。

AI3

3 技術基盤の取得と保守

3.1 新しいハードウェアとソフトウェアの評価

コントロール目標

新しいハードウェアとソフトウェアが全体システムの性能に与える影響について評価する手続があること。

3.2 ハードウェアに関する予防保全

コントロール目標

情報サービス機能の管理者は，性能上の不具合の頻度と影響を軽減するために，日常的かつ定期的な保守を予定すること。

3.3 システム･ソフトウェアのセキュリティ

コントロール目標

情報サービス機能の管理者は，導入予定のシステム･ソフトウェアの装備が，システムに保存されたデータとプログラムのセキュリティを損なわないことを保証すること。システム･ソフトウェアのパラメータの準備と保守に注意が払われること。

3.4 システム･ソフトウェアの導入

コントロール目標

システム･ソフトウェアが技術基盤の取得と保守フレームワークに従って導入されていることを保証するために，手続が設けられること。テストは，本番環境での利用が承認される前に実施されること。

3.5 システム･ソフトウェアの保守

コントロール目標

システム･ソフトウェアが技術基盤の取得と保守のフレームワークの従って，保守されていることを保証するために，手続が設けられること。

3.6 システム･ソフトウェアの変更管理

コントロール目標

システム･ソフトウェアの変更が組織の変更管理の手続に沿って，コントロールされていることを保証するために，手続が設けられること。

AI4

4 ITシステム関連手続の作成と保守

4.1 将来の運用要件とサービス水準

コントロール目標

組織のシステム開発ライフサイクル方法論は，将来の運用要件およびサービス水準について適時に定義することを保証すること。

4.2 ユーザ手続マニュアル

コントロール目標

組織のシステム開発ライフサイクル方法論は，適切なユーザ手続マニュアルが作成され，各情報システムの開発，実施または改訂プロジェクトの一部として作成され，見直しされることを規定すること。

4.3 運用マニュアル

コントロール目標

組織のシステム開発ライフサイクル方法論は，適切な運用マニュアルが作成され，各情報システムの開発，実施または改訂プロジェクトの一部として作成され，更新されることを規定すること。

4.4 教育資料

コントロール目標

組織のシステム開発ライフサイクル方法論は，適切な教育資料が各情報システムの開発，実施または改訂プロジェクトの一部として，作成されることを規定すること。これらの資料は，日常業務のシステム利用に焦点が当てられること。

AI5

5 システムの認証と導入

5.1 教育

コントロール目標

影響を受けるユーザ部門と情報サービス機能の運用グループのスタッフが，情報システム開発，実施または改訂プロジェクトの一部として明示された教育計画と関連資料に従って教育されること。

5.2 性能最適化の適用

コントロール目標

アプリケーション・ソフトウェアの性能のサイジング（最適化）は，新しく，かつ，大幅に変更されたソフトウェアに対して要求される資源を予測するために，組織のシステム開発ライフサイクル方法論の不可欠な部分として確立されること。

5.3 移行

コントロール目標

組織のシステム開発ライフサイクル方法論は，各情報システム開発，実施または改訂プロジェクトの一部として，予め作成された計画に基づいて旧システムからの必要な要素が新システムの要素として変換されることを盛り込むこと。

5.4 変更テスト

コントロール目標

管理者は，通常のデータ運用環境における利用を開始する前に，独立した（構築者から）テストグループによって別個のテスト環境における影響と資源の評価に従って，変更がテストされることを保証すること。撤退計画もまた，作成されること。検収テストは，将来の運用環境（例えば，類似のセキュリティ，内部統制，負荷など）を代表するような環境で実施されること。

5.5 並行／パイロットテストの基準と性能

コントロール目標

並行またはパイロットテストが予め作成された計画に従って実施され，このテスト・プロセスの終了基準が前以って明記されていることを保証する適切な手続があること。

5.6 最終検収テスト

コントロール目標

新しいまたは改訂情報システムの品質保証の最終検収または品質保証テストの一部として，影響を受けるユーザ部門と情報サービス機能の管理者によるテスト結果の正式の評価と承認手続が必要である。テストは，情報システムの全ての要素（アプリケーション・ソフトウェア，設備，技術，ユーザ手続）を網羅すること。

5.7 セキュリティテストと認証

コントロール目標

管理者は，運用とユーザ管理者が正式にテスト結果および残余のリスクを考慮したシステムのセキュリティのレベルを受容することを保証するための手続を明示し，実施すること。

5.8 運用テスト

コントロール目標

システムを運用段階に移行する前に，ユーザまたは任命されたカスタディアン（ユーザの代わりにシステ

ムを運営するために任命された関係者）は，アプリケーション環境に類似する状況の下で，システムが本番環境で運用されるような方法で，完全な製品としての運用を検証することを保証すること。

5.9 本番への移行

コントロール目標

管理者は，開発から運用へのテストの引き継ぎを統制する正式な手続を明示し，実施すること。各々の環境は分離され，適切に保護されること。

5.10 ユーザ要件の適合度評価

コントロール目標

組織のシステム開発ライフサイクル方法論は，運用中の情報システムの要件（例　キャパシティ，スループットなど）の導入後レビューが，ユーザニーズがシステムによって達成されつつあるかどうかを評価するために，実施されるよう要求すること。

5.11 管理者による導入後レビュー

コントロール目標

組織のシステム開発ライフサイクル方法論は，運用中の情報システムの導入後のレビューを行って，システムが最もコスト効果のある方法でもくろんだ効果を確保しているかを評価し，報告をすることを盛り込むよう要求すること。

AI6

6 変更管理

6.1 変更要求の開始とコントロール

コントロール目標

管理者は，変更，システム保守および供給者の保守に対するの全ての要求が標準化され，公式の変更管理手続に従っていることを保証すること。変更は分類され，優先順位付けされ，緊急の問題を処理する適切な特定の手続がなければならない。変更要求者は，その要求の処理状況を知らされること。

6.2 影響の評価

コントロール目標

変更のすべての要求は，運用システムとその機能への可能な全ての影響について，構造化された方法で評価されることを保証する適切な手続がなければならない。

6.3 変更の管理

コントロール目標

管理者は，変更管理，ソフトウェア･コントロールおよび配付は，包括的な構成管理システムに適切に統合化されることを保証すること。

6.4 文書化と手続

コントロール目標

変更プロセスは，システム変更が実施されるときはいつでも，関連文書と手続がそれに従って更新されることを保証すること。

6.5 権限付与された保守の承認

コントロール目標

管理者は，保守要員が特定の任務をもち，その業務が適切にモニターされることを保証すること。さらに，彼らのシステムのアクセス権限が，自動化システムへの不正アクセスというリスクを回避するために統制されること。

6.6 ソフトウェアのリリース方針

コントロール目標

管理者は，ソフトウェアのリリースが署名，包装，復帰テストおよび引き継ぎなどを保証する正式な手続によって管理されることを保証すること。

6.7 ソフトウェアの配付

コントロール目標

適切な監査証跡を伴って，インテグリティ，そして適時的に正しい場所への正確なソフトウェア要素の配付を保証するために，特定の内部統制の対策が確立されること。

DS1

1 サービスレベルの定義

1.1 サービスレベル合意書のフレームワーク

コントロール目標

上級管理者は，フレームワークが正式なサービスレベル合意書の定義を促進し，最小限の内容をを定義するフレームワークを定義すること。最小限の内容とは，可用性，信頼性，性能，拡張の可能性，ユーザに提供される支援レベル，継続性計画，セキュリティ，満足なデリバリされたシステム機能の最小限の受容レベル，制約（業務量の限界），サービス料金，中央のプリント設備（可用性），中央のプリントの配付，変更手続である。ユーザと情報サービス機能は，定性的および定量的な表現で，サービスレベルを記述する合意書をもつこと。合意書は，両者の責任を定義する。情報サービス機能は，合意されたサービスの品質と量を提供しなければならない，また，ユーザは，合意された限界の中でサービスの要求を制限しなければならない。

1.2 サービスレベル合意書の内容

コントロール目標

サービスレベル合意書がもたなければならない項目に関する明白な合意がされること。サービスレベル合意書は，少なくとも次の項目を網羅すること。すなわち，可用性，信頼性，性能，拡張の可能性，ユーザに提供される支援レベル，継続性計画，セキュリティ，満足なデリバリされたシステム機能の最小限の受容レベル，制約（業務量の限界），サービス料金，中央のプリント設備（可用性），中央のプリントの配付および変更手続である。

1.3 性能手続

コントロール目標

影響を受けるすべての部門に対して，関与する関係者全ての間の業績を左右する関係（例　非開示の合意）に対する方法と責任を確立し，調整し，維持する手続がなければならない。

1.4 モニタリングと報告

コントロール目標

情報サービス機能の管理者は，明記されたサービス機能標準の達成と処理中に生じた問題全てに関するモニタリングと報告に責任があるサービスレベル管理者を任命すること。モニタリングの統計は，適時に分析されること。適切な是正行動がとられ，不具合は調査されること。

1.5 サービスレベル合意書と契約書のレビュー

コントロール目標

管理者は，サービスレベル合意書と第三者機関のサービス･プロバイダとの補強契約について定期的なレビュー･プロセスを設けること。

1.6 課金項目

コントロール目標

課金項目の条項は，サービスレベルとコストを比較し，釣り合いをとれるようにするために，サービスレベル合意書に含まれること。

1.7 サービス向上プログラム

コントロール目標

管理者は，ユーザとサービスレベル管理者がサービスレベルに対してコスト面で正当化された改善を追求するサービス向上計画に定期的に合意することを保証するプロセスを設けること。

DS2

2 第三者機関のサービスの管理

2.1 供給者とのインタフェース

コントロール目標

管理者は，第三者機関のプロバイダのサービス全てが適切に識別され，供給者との技術的および組織的インタフェースが文書化されていることを保証すること。

2.2 オーナとの関係

コントロール目標

顧客の組織管理者は，第三者機関との関係の品質を保証する責任がある関係オーナーを任命すること。

2.3 第三者機関との契約書

コントロール目標

管理者は，それぞれの第三者機関のサービス･プロバイダとの関係において，正式な契約が明示され，合意されていることを保証するために，特定の手続を明示すること。

2.4 第三者機関の適格性

コントロール目標

管理者は，選択に先立って，潜在的な第三者機関が，必要となるサービス（十分な注意義務）を提供する能力の評価を通じて，全く的確であることを保証すること。

2.5 アウトソーシング契約書

コントロール目標

特定の組織手続が，設備管理業者と組織間の契約が，要求された処理レベル，セキュリティ，モニタリングとコンティンジェンシー要件および適切な他の規制に基づいていることを保証するために，明示されること。

2.6 サービスの継続

コントロール目標

サービスの継続性を保証することに関して，管理者は第三者機関の法的な不安と継続企業概念の点で第三者機関に関連するビジネスリスクを考慮し，適切な場合には条件付契約を取り決めること。

2.7 セキュリティとの関係

コントロール目標

第三者機関のサービス･プロバイダとの関係について，管理者は，セキュリティ合意書（例　非開示合意書）が識別され，法的および責任を含む規制要件に従って，明確に述べられ，合意され，普遍的なビジネス基準に準拠していることを保証すること。

2.8 モニタリング

コントロール目標

第三者機関のサービス･デリバリの継続的なモニタリングプロセスは，契約書に準拠していることを確保するために，管理者によって設定されること

DS3

3 性能とキャパシティの管理

3.1 可用性と性能要件

コントロール目標

管理プロセスは，ビジネスニーズが情報サービスの可用性と性能に関して識別され，可用性の条件と要件に引き直されていることを保証すること。

3.2 可用性の計画

コントロール目標

管理者は，情報サービスの可用性を達成し，モニタリングし，コントロールする可用性計画の確立を保証すること。

3.3 モニタリングと報告

コントロール目標

管理者は，IT資源の性能が継続してモニタリングされ，例外が適時にかつ理解できる方法で報告されていることを保証するために，プロセスを導入すること。

3.4 モデリング･ツール

コントロール目標

管理者は，実際の負荷に対して修正され，調整され，かつ推奨された負荷レベルの範囲において正確である現行システムのモデルを作るために，適切なモデリング･ツールが使用されることを保証すること。モデリング･ツールは，キャパシティの予測，構成の信頼性，性能と可用性の要件を支援するために使用されること。深い技術調査が，システム･ハードウェアについて実施され，将来の技術に関する予測を含むこと。

3.5 積極的な性能管理

コントロール目標

性能管理プロセスは，問題がシステム性能に影響する前に修正できるように，予測能力を含むこと。分析は，頻度，影響の程度，損失額に関して，システムの不具合と異常について実施されること。

3.6 負荷の予測

コントロール目標

コントロールは，傾向を識別し，キャパシティ計画に必要な情報を提供するために，負荷予測が作成されることを保証するために適切でなければならない。

3.7 資源のキャパシティ管理

コントロール目標

情報サービス機能の管理者は，コスト的に正当化できるキャパシティが，合意された負荷を処理し，サービスレベル合意書で要求された性能品質と数量を提供すべく，常に存在することを保証するために，ハードウェア性能とキャパシティのレビューに関する計画策定プロセスを確立すること。キャパシティ計画は，多様なシナリオを網羅すること。

3.8 資源の可用性

コントロール目標

管理者は，フォルトトレランスの機構，タスクの優先度付け，そして，公正な資源配置機構の導入により，資源が利用できなくならないようにすること。

3.9 資源のスケジュール

コントロール目標

管理者は，回復力，コンティンジェンシー，負荷およびストレージ計画のような側面を考慮して，必要キャパシティの適時な取得を保証すること。

DS4

4 継続的サービスの保証

4.1 IT継続性のフレームワーク

コントロール目標

情報サービス機能の管理者は，役割，責任，採用されるべきリスクベースアプローチ／方法論，そして，承認手続とともに計画を文書化する規則と構造を定める，継続性フレームワークを策定しなければならない。

4.2 IT継続性計画の戦略と原理

コントロール目標

管理者は，IT継続性計画が，一貫性を保証するために，全体的な業務継続性計画と調和していることを保証すること。さらに，IT継続性計画は，一貫性を確保するために，ITの長期および中期の計画を考慮すること。

4.3 IT継続性計画の構成要素

コントロール目標

情報サービス機能の管理者は，以下を含む文書化された計画が策定されることを保証すること。

- －継続性計画の利用方法についてのガイドライン
- －すべての関連する職員の安全を保証する緊急時手続
- －事故または災害以前の状態に業務を復帰させるという意味のレスポンス手続
- －事故または災害以前の状態に業務を復帰させるという意味の復旧手続
- －ホームサイトを保護し再構築する手続
- －公共機関と調整する手続
- －利害関係者（従業員，主要な顧客，重要な供給業者，株主および管理者）に伝達する手続
- －継続性チーム，関連スタッフ，顧客，供給業者，公共機関およびメディアについての重要情報

4.4 IT継続性要件の最小化

コントロール目標

情報サービス機能の管理者は，人員，設備，ハードウェア，ソフトウェア，装置，用紙，消耗品，および，什器に関する継続性要件を最小化するための手続とガイドラインを策定すること。

4.5 IT継続性計画の保守

コントロール目標

情報サービス機能の管理者は，継続性計画が最新の状態であることと，現在の業務要件を反映していることを保証するために変更コントロール手続を提供すること。このことは，継続性計画の保守手続が，変更と管理および人的資源の手続と調整されることを要求する。

4.6 IT継続性計画のテスト

コントロール目標

有効な継続性計画を持つために，管理者は定期的にその妥当性を評価すること。このことは，注意深い準備，文書化，テスト結果の報告，そして，その結果に基づいた活動計画の実施を要求する。

4.7 IT継続性計画の訓練

コントロール目標

障害時継続性方法論は，関係者全てが，事故や災害時に従わなければならない手続について，定期的な訓練セッションを受けることを確保すること。

4.8 IT継続性計画の配付

コントロール目標

継続性計画に含まれる情報が機密の性質を持つことから，継続性計画は，承認された人だけに配付される必要があり，承認されない開示に対して保護されること。従って，計画のセクションは，業務上の必要性（need-to-know）原則に従って配付されること。

4.9 ユーザ部門における代替処理バックアップ手続

コントロール目標

継続性方法論は，ユーザ部門が情報サービス機能が災害や事象の後，そのサービスを復旧できるまで利用できる代替処理手続を確立することを保証すること。

4.10 重要なIT資源

コントロール目標

継続性計画は，災害の発生後，復旧に必要な重要なアプリケーション・プログラム，第三者機関のサービス，オペレーティング・システム，要員と消耗品，データ・ファイル，および時間枠を識別すること。

4.11 バックアップ・サイトとハードウェア

コントロール目標

管理者は，継続性計画が最終の代替案選択とともに，バックアップ・サイトとハードウェアに関して，代替案の識別を組入れていることを保証すること。適用できるなら，これらの種類のサービスの正式な契約書を締結していること。

4.12 終結手続

コントロール目標

災害後に，情報サービス機能の再開が成功するには，情報サービス機能の管理者は，計画の適切性を保証する手続を確立し，これに従って計画を改訂すること。

DS5

5 システムセキュリティの保証

5.1 セキュリティ対策の管理

コントロール目標

ITセキュリティは，セキュリティ対策が業務要件と整合するように管理されること。このことは，以下のことを含む。

－リスク評価情報のITセキュリティ計画への反映
－ITセキュリティ計画の実施
－IT構成の変化を反映したITセキュリティ計画の変更
－ITセキュリティについての変更要求の影響の評価
－ITセキュリティ計画の実施の監視
－ITセキュリティ手続と他の方針や手続との調整

5.2 識別，認証とアクセス

コントロール目標

情報サービス機能の計算資源への論理的アクセスと使用は，アクセスルールに関連する利用者と資源を識別する適切な認証機構の導入によって制限されること。そのような機構は，不許可の要員，ダイアルアップ接続および他のシステム（ネットワーク）エントリー・ポートからのコンピュータ資源へのアクセスを防止し，許可されたユーザが多重サインオンを使用する必要性を最小にすること。手続は，また，認証とアクセス機構を有効に（例　定期的なパスワード変更）保持するために適切でなければならない。

5.3 データへのオンライン・アクセスのセキュリティ

コントロール目標

オンラインのIT環境において，情報サービス機能の管理者は，個人の明示されたデータを見たり，追加したり，変更したり，または削除する必要性に基づいて，アクセス・セキュリティ・コントロールを提供するセキュリティ方針に沿って，手続を導入すること。

5.4 ユーザアカウントの管理

コントロール目標

管理者は，ユーザアカウントの申請，登録，発行，保留，一時停止および閉鎖に関連する適時な行動を保証する手続を作成すること。データまたはシステム・オーナがアクセス特権を許可することを略述する正式な承認手続を含めること。

5.5 ユーザアカウントの管理者レビュー

コントロール目標

管理者は，アクセス権限を定期的にレビューし，確認するための適切なコントロール・プロセスを有すること。

5.6 ユーザアカウントのユーザコントロール

コントロール目標

ユーザは，その独自のアカウントに関わる行為を組織的にコントロールすること。また，ユーザが異常な行為について適時に警告されるとともに，通常の活動を監督することもできるように，情報機構がなければならない。

5.7 セキュリティ監視

コントロール目標

情報サービス機能のセキュリティ管理者は，セキュリティ行為のログが取られ，際迫ったセキュリティ侵害の兆候が直ちに管理者に知らされ，自動的に対応行動が行われることを保証すること。

5.8 データ分類

コントロール目標

管理者は，データ分類スキームに従って，データ･オーナによる正式かつ明示の決定によって，データ全てが機密度の観点から分類されていることを保証する手続を実施すること。「保護しない」とされるデータでさえ，そのように指定する旨の正式な決定を必要とする。

5.9 識別とアクセス権限の集中管理

コントロール目標

全体のアクセス･コントロールの一貫性と効率性を得るために，システムとデータ･オーナーシップの主体性と同様，ユーザの識別およびアクセス権限が確立され，一意的かつ集中した方法で管理することを保証するために，適切なコントロールがあること。

5.10 違反とセキュリティ活動の報告書

コントロール目標

情報サービス機能のセキュリティ管理者は，違反とセキュリティ活動が不正活動を含む事象を識別し，解決するために定期的にログされ，報告され，レビューされ，適切に上申されていることを保証すること。コンピュータ資源の説明情報（セキュリティと他のログ）への論理的アクセスは，最少維持，つまり，業務上の必要性の原理に基づいて許可されること。

5.11 障害の処理

コントロール目標

管理者は，十分な専門家と迅速で安全な通信施設を備えた集中プラットフォームを提供することによって，セキュリティ障害に対処するコンピュータ･セキュリティ障害処理能力を確立すること。障害の管理責任と手順は，セキュリティ障害に対して，適切で有効で秩序ある対応を保証するために確立されること。

5.12 再認定

コントロール目標

管理者は，セキュリティの再認定（例「タイガーチーム」によって）が，正式に承認されたセキュリティ･レベルと残余のリスクの受容を最近の状態に保つために定期的に実施されること。

5.13 取引相手の信用

コントロール目標

組織の方針は，取引相手の提供する電子的な指示や取引の真正性を確認するために，コントロール実務が導入されることを保証すること。これは，パスワード，トークン，または暗号鍵の信頼できる交換によって実現することができる。

5.14 取引の認証

コントロール目標

組織の方針は，適切な場合には，取引の真正性を提供するためにコントロールが導入されることを保証すること。これは，署名と取引確認のために暗号技術を利用することを要求する。

5.15 否認防止

コントロール目標

組織の方針は，適切な場合には，取引が当事者双方により拒否できないこと，そして，発信者または受信者の否認防止，取引実行の証拠，取引の受信確認を提供するためにコントロールが導入されること，を保

証すること。

5.16 信頼できる経路

コントロール目標

組織の方針は，機密の取引データが信頼できる経路を通じてのみ交換されることを保証すること。機密の情報には，セキュリティ管理情報，機密の取引データ，パスワード，および，暗号鍵が含まれる。これを実現するには，ユーザ間，ユーザとシステム間，そしてシステム間で，暗号を利用して信頼できるチャネルを確立する必要もあろう。

5.17 セキュリティ機能の保護

コントロール目標

セキュリティに関連するすべてのハードウェアとソフトウェアは，いかなる時においても，そのインテグリティの維持に対する不正な変更，および秘密鍵の開示から保護されること。さらに，組織は，そのセキュリティ設計を目立たないように保持することが，組織のセキュリティをその秘密とされる設計に基づかせてはならない。

5.18 暗号鍵の管理

コントロール目標

管理者は，改竄と不正開示に対して鍵の保護を保証するために，暗号化鍵の生成，配付，認証，保管，入力，使用，収容に使用される手順とプロトコルを明示し，実施すること。もし，鍵の信用がなくなったならば，管理者は，その情報が認証失効リスト（CRL）や同様の機構の利用を通じて，関連するいかなる当事者に対しても伝えられることを保証すること。

5.19 不当ソフトウェアの予防，発見，復旧

コントロール目標

コンピュータ・ウィルスやトロイの木馬のような不当ソフトウェアに関連して，管理者は，適切な予防，発見および復旧のコントロール手段のフレームワークを確立すること。

5.20 ファイヤウォールアーキテクチャーと公共ネットワークへの接続

コントロール目標

インターネットや他の公共ネットワークへの接続が存在しているならば，適切なファイヤーウォールの運営により，サービスの停止および内部資源への権限のないアクセスから保護される必要があり，いかなるアプリケーションと基盤の管理フローを双方向でコントロールする必要があり，そして，攻撃によるサービスの停止に対して保護されること。

5.21 電子的価値の保護

コントロール目標

管理者は，認証や，財務または機密の情報の記憶に使われるすべてのカードや同様の物理的装置の継続的なインテグリティを，関連する機器，デバイス，従業員，および使用される確認方法を考慮して，保護すること。

DS6

6 コストとの識別と賦課

6.1 課金項目

コントロール目標

情報サービス機能の管理者は，課金対象項目がユーザによって識別，測定および予測できることを保証すること。ユーザは，情報サービスの利用と関連した請求レベルをコントロールできなければならない。

6.2 原価計算手続

コントロール目標

情報サービス機能の管理者は，コスト有効性を確保しながら，情報サービスをデリバリするコストに関する管理情報を提供するために，コスト手続を明示し，実施すること。予測と実際コストの間の差異は，コストモニタリングを行うために適切に分析され，報告されること。さらに，上級管理者は，組織の他の会計測定システムに照らして，情報サービス機能のジョブコスト会計手続の結果を定期的に評価すること。

6.3 ユーザへの請求と課金手続

コントロール目標

情報サービス機能の管理者は，請求と課金手続を明示し，使用すること。情報サービス機能の管理者は，コンピュータ資源の適切な利用を促進し，ユーザ部門とそれらのニーズとの適正な処理を保証するユーザ請求と課金手続を維持すること。課金率は，サービスを提供する関連コストを反映すること。

DS7

7 ユーザの教育と訓練

7.1 教育の必要性の識別

コントロール目標

長期計画に基づいて，管理者は，情報サービスを活用する要員全ての教育ニーズを識別し，文書化する手順を作成し，維持すること。従業員の各グループの教育カリキュラムが作成されること。

7.2 教育組織

コントロール目標

識別されたニーズに基づいて，管理者は目標とするグループを定義し，教育者を識別し，任命し，適時な教育セッションを編成すること。代替的な教育も，また調査（内部または外部の場所，社内の講師または第三者機関の講師）されること。

7.3 セキュリティの原則と意識教育

コントロール目標

要員全ては，システム・セキュリティ原則について訓練され，教育されること。上級管理者は，以下を含む教育，研修プログラムを提供すること。それらは，情報サービス機能の倫理綱領，および可用性，機密性，インテグリティ，安全な方法による業務の実施に影響を与える障害から損傷に対して保護するセキュリティの慣行である。

DS8

8 ITのカスタマへの支援と助言

8.1 ヘルプデスク

コントロール目標

「ヘルプデスク」機能の内で，ユーザ支援が確立されること。この機能の実施責任者は，問題管理の要員と緊密に連絡し合うこと。

8.2 カスタマ照会の登録

コントロール目標

カスタマからの照会は全て，適切にヘルプデスクによって登録されることを保証するために，適切な手続がなければならない。

8.3 カスタマ照会の上申

コントロール目標

ヘルプデスクによって直ちに解決できないカスタマからの照会が，情報サービス機能内で適切に上申されるヘルプデスク手続が必要である。

8.4 照会回答済みのモニタリング

コントロール目標

管理者は，カスタマ照会の処理済みを適時にモニタリングする手続を作成すること。長期の未解決の照会は，調査され，対処されること。

8.5 傾向の分析と報告

コントロール目標

カスタマの照会と解決，レスポンスタイムと傾向の識別に関する適切な報告を保証する適切な手続がなければならない。報告書は，適切に分析され，対処されること。

DS9

9 構成管理

9.1 構成の記録

コントロール目標

許可され，識別可能な構成項目だけが取得に当たって一覧表に記録されることを保証するために，適切な手続がなければならない。これらの手続は，承認された廃棄および結果として生じる構成品目の売却についても規定していること。さらに，構成の変更記録（新規項目，開発からプロトタイプへの状況変更）を取る適切な手続がなければならない。ロギングとコントロールは，変更した記録のレビューを含む，統合化された構成記録システムの一部でなければならない。

9.2 構成のベースライン

コントロール目標

情報サービス機能の管理者は，構成項目のベースラインが変更後へ戻るためのチェックポイントとして維持されていることを保証すること。

9.3 状況の説明

コントロール目標

情報サービス機能の管理者は，構成記録が変更の履歴を含む構成項目の全ての実際の状態を反映していることを保証すること。

9.4 構成のコントロール

コントロール目標

情報サービス機能の構成記録の実在性と一貫性が定期的にチェックされることを，手続は保証すること。

9.5 違法ソフトウェア

コントロール目標

情報サービス機能の管理者は，違法なソフトウェアについて組織のパーソナル・コンピュータを定期的にチェックすること。

9.6 ソフトウェアの保管

コントロール目標

ファイル・ストレージ・エリア（ライブラリ）は，システム開発ライフサイクルの適切な局面において，有効なソフトウェア項目全てについて明示されること。これらの領域は，相互に，および開発，テスト，本番ファイルストレージ領域から分離されること。

DS10

10 問題と障害管理

10.1 問題管理システム

コントロール目標

情報サービス機能の管理者は，標準オペレーションの一部でない運用の事象（障害，問題とエラー）全てが適時に記録され，分析され，解決されていることを保証するために，問題管理システムを明示し，実施すること。障害の報告書は，重大な問題が発生した場合，作成されること。

10.2 問題の上申

コントロール目標

管理者は，識別された問題が適時に最も効率的な方法で解決されることを保証するために，問題上申手続を明示し，実施すること。これらの諸手続は，優先度が適切に設定されていることを保証すること。その手続は，IT継続計画が発効された際の上申手続も文書化すること。

10.3 問題の追跡と監査証跡

コントロール目標

問題管理システムは，障害から根本的な原因（例　パッケージ・リリースまたは緊急変さらによる導入）を跡付けられる適切な監査証跡を提供すること。それは，変更管理，可用性管理および構成管理と緊密に機能すること。

DS11

11 データ管理

11.1 データ作成の手続

コントロール目標

管理者は，ユーザ部門によって遵守されるべきデータの作成手続を作成すること。この趣旨は，エラーと脱落が最小にされることを保証するために入力フォームの設計が役立つこと。データ作成中のエラー処理手続は，エラーと異常が検出され，報告され，修正されることを合理的に保証すること。

11.2 原始ドキュメントの承認手続

コントロール目標

管理者は，原始書類が権限内で執行する認可された要員だけによって適切に作成され，原始書類の起案と承認について適切な職務の分離がされていることを保証すること。

11.3 原始ドキュメントのデータ収集

コントロール目標

組織の手続は，承認された全ての原始資料は完全で，正確で，適切に説明可能で，入力について適時に送達されることを保証すること。

11.4 原始ドキュメントエラーの取扱

コントロール目標

データ作成中のエラー処理手続は，エラーと異常が検出され，報告され，修正されることを合理的に保証すること。

11.5 原始ドキュメントの保存

コントロール目標

原始書類が，法的要件を満たすのとともに，データの検索または再構築が適切な時間によって可能な組織によって保管され，あるいは再生可能であることを保証する適切な手続がなければならない。

11.6 データ入力承認手続

コントロール目標

組織は，データ入力が許可されたスタッフだけによって実施されることを保証するために，適切な手続を作成すること。

11.7 正確性，完全性および承認チェック

コントロール目標

処理のために入力されたトランザクションデータ（人々によって作成された，システムによって生成された，またはインターフェイス入力）は，正確性，完全性および妥当性をチェックする多様なコントロールに従うこと。手続は，また，入力データが可能な限り，発生点の近くで検証され，誤謬摘示されることを保証するために作成されること。

11.8 データ入力エラーの処理

コントロール目標

組織は，過って入力されたデータの修正と再入力の手続を作成すること。

11.9 データ処理のインテグリティ

コントロール目標

組織は，職務の分離が維持され，実施された業務が定期的に検証されていることを保証するデータ処理の手続を作成すること。手続は，ラン･ツー･ラン･コントロール･トータル，マスタ･ファイル更新コントロールのような適切な更新コントロールを保証すること。

11.10 データ処理の妥当性と誤謬摘示

コントロール目標

組織は，データ処理の検証，認証，誤謬摘示が可能な限り，発生点に近くで実施されることを保証する手続を作成すること。人工知能(AI)システムが使われている場合には，それらのシステムは，重要な決定が承認を受けることを保証するために，人間の操作員との双方向のコントロールフレームワークの中におかれること。

11.11 データ処理エラーの取扱

コントロール目標

組織は，誤りのあるトランザクションが処理されないで，また，他の妥当なトランザクションの処理の不当な障害なく，識別できるデータ処理エラー取扱手続を作成すること。

11.12 出力の取扱と保存

コントロール目標

組織は，ITによるアプリケーション･プログラムからの出力の取扱いと保存の手続を作成すること。流通証券（例，バリューカード）が出力である場合には，悪用から保護されるために特別の注意が払われること。

11.13 出力の配付

コントロール目標

組織は，ITによる出力の配付についての書面による手続を作成し，伝達すること。

11.14 出力の合計突合と照合調整

コントロール目標

組織は，日常的な出力が関連のあるコントロール･トータルとバランスしていることを保証する手続を作成すること。監査証跡は，トランザクション処理と中断したデータの照合調整の追跡ができるように提供されること。

11.15 出力のレビューとエラーの取扱

コントロール目標

組織の管理者は，出力報告書の正確性が提供者と関連ユーザによってレビューされることを保証する手続を作成すること。出力に含まれるエラーをコントロールする適切な手続もなければならない。

11.16 出力報告書のセキュリティ条項

コントロール目標

組織は，ユーザに既に配付されたものとともに，配付予定の出力報告書のセキュリティが維持されることを保証する手続を作成すること。

11.17 伝送と輸送中における機密情報の保護

コントロール目標

管理者は，不正なアクセス，改竄および誤配送に対して，機密情報の適切な保護が伝送中および輸送中になされていることを保証すること。

11.18 廃棄機密情報の保護

コントロール目標

管理者は，廃棄された機密組織情報の非開示を保証する手続を定義し，導入すること。そのような手続は，削除済みあるいは廃棄予定と示されたデータが，いかなる内部または第三者機関によっても検索できないことを保証すること。

11.19 保管管理

コントロール目標

手続は，検索要件，そして，費用効果とセキュリティ方針を考慮するデータの保管について作成すること。

11.20 保存期間と保管条件

コントロール目標

保管期間と保管条件は，ドキュメント，データ，プログラムおよび報告書とメッセージ（受信と送信）について，それらの暗号化および認証に使用されるデータ（鍵，認証書）とともに明示されること。

11.21 媒体ライブラリ管理システム

コントロール目標

情報サービス機能は，データを含む媒体ライブラリの内容が体系的に目録が作成され，物理的在庫品調べによって明らかにされた差異が適時に修正され，ライブラリに保管された磁気媒体のインテグリティを維持するために対策が取られることを保証する手続を作成すること。

11.22 媒体ライブラリ管理の責任

コントロール目標

媒体ライブラリの内容を保護するために設計された管理維持手続は，情報サービス機能の管理者によって作成されること。基準は，説明責任を支援するために，磁気媒体の外部識別，物理的移動および保管のコントロールのために定義されなければならない。媒体（磁気テープ，カートリッジ，ディスクとディスケット）ライブラリの管理責任は，情報サービス機能の特定メンバーに割り当てられること。

11.23 バックアップと復旧

コントロール目標

管理者は，バックアップと復旧の適切な戦略を策定し，復旧計画の開発，導入，テスト，文書化とともに，ビジネス要件のレビューがそれに含まれることを保証すること。手続は，バックアップが上述した要件を満たすことを保証するために設定されること。

11.24 バックアップ・ジョブ

コントロール目標

バックアップが定義されたバックアップ戦略に従って実施されるのを保証する適切な手続が必要であり，バックアップの使用可能性が定期的に検証されるべきである。

11.25 バックアップ保管

コントロール目標

ITの関連媒体のバックアップ手続は，オンサイトとオフサイトの両方で，データ・ファイル，ソフトウェアと関連する文書の適切な保管を含むこと。バックアップは，安全に保管され，保管サイトは，物理的アクセス・セキュリティとデータ・ファイルと他の項目のセキュリティに関して，定期的にレビューされること。

11.26 保管

コントロール目標

管理者は，アーカイブにあるものが，法律とビジネスの要件に適合し，適切に保護され，説明される状態にあることを保証する方針と手続を実施すること。

11.27 機密メッセージの保護

コントロール目標

インターネットや他の公共ネットワークを通じてデータが伝達されることに関し，管理者は，機密メッセージのインテグリティ，秘密性，および，否認拒否を保証するために使用されるべき手続とプロトコルを明示し，実施すること。

11.28 認証とインテグリティ

コントロール目標

電話，ボイスメール，紙の文書，ファックス，または，電子メールによって受信された，組織の外部から発信された情報の認証とインテグリティは，潜在的に重要な行為が行われる前に適切にチェックされること。

11.29 電子取引のインテグリティ

コントロール目標

時間や地理上の伝統的な境界が信頼性を失っていくことを考慮し，管理者は，機密または重要な電子取引について，以下のインテグリティと真正性を保証するため，適切な手続と実施を明示し，実施すること。

- 原子性（作業の個々の単位，その活動のすべてが成功するか失敗するかいずれかである）
- 整合性（もし，取引が安定した終了状態にならないならば，システムをその初期状態に戻さなければならない）
- 分離（取引の行動が，並行して実行される他の取引に影響を受けない）
- 永続性（取引の効果が，それがコミットされた後に永続しており，その変更がシステムの故障に耐える）

11.30 記憶データの継続的なインテグリティ

コントロール目標

管理者は，ファイルやその他の媒体（例，電子カード）に保持されたデータのインテグリティと正確性が定期的にチェックされることを保証すること。特別な注意が，バリュートークン，参照ファイル，およびプライバシー情報を含むファイルに対して向けられること。

DS12

12 ファシリティ管理

12.1 物理的セキュリティ

コントロール目標

情報設備のオフサイト利用を含むIT設備に対する適切な物理的セキュリティとアクセス・コントロール対策は，全般セキュリティ方針に準拠して作成されなければならない。アクセスは，そのアクセスができる認可された個人に制約されること。

12.2 目立たないITサイト

コントロール目標

情報サービス機能の管理者は，目立たず，ITの運用サイトの物理的な識別が制限されることを保証すること。

12.3 訪問者への付添

コントロール目標

情報サービス機能の運用グループのメンバーでない者は，コンピュータ施設に入らなければならない時，そのグループのメンバーによって付き添われることを確保する適切な手続がなければならない。訪問者の記録は保存され，定期的にレビューされること。

12.4 要員の健康と安全

コントロール目標

健康と安全の慣行は，適用可能な国際的，国内，地域，州，条例および規制に従って適切に実施され，維持されること。

12.5 環境要因に対する保護

コントロール目標

情報サービス機能の管理者は，環境要因（例　火災，埃，電力，過剰の熱と湿度）からの保護のために十分な対策が適切に行われ，維持されることを保証すること。環境を監視し，コントロールする特殊な設備と機器が設置されること。

12.6 無停電電源装置

コントロール目標

管理者は，電力の障害と変動に対し，重要なITのアプリケーションを確保するために，無停電電源装置の蓄電池と発電機の必要性を定期的に評価すること。必要な場合は，最も適切な設備が設置されること。

DS13

13 運用管理

13.1 処理運用手続と教育マニュアル

コントロール目標

情報サービス機能は，ITの運用（ネットワーク運用を含む）の標準手続を確立し，文書化すること。ITの解決策と基盤は全て，これらの手続を用いて適切に運用され，これらの手続は，有効性と準拠性を保証するために定期的にレビューされること。

13.2 開始プロセスと他の運用文書

コントロール目標

情報サービス機能の管理者は，運用スタッフによって，開始プロセスと他の運用タスクが文書化され，定期的にテストされ，必要に応じて調整されることによって，十分に精通し，自身があることを保証すること。

13.3 ジョブ･スケジューリング

コントロール目標

情報サービス機能の管理者は，サービス･レベル合意書で設けられた目標を満たすために，スループットと利用度を最大にしながら，最も効率的な順番で組織化されたジョブ，プロセス，およびタスクの継続的スケジュールを保証すること。当初のスケジュールは，スケジュールへの変更とともに適切に承認されること。

13.4 標準ジョブ･スケジュールとの差異

コントロール目標

標準のジョブ･スケジュールからの乖離を識別し，調査し，承認する適切な手続がなければならない。

13.5 処理の継続

コントロール目標

手続は，正式の活動の引継ぎ，状況の更新，現行の責任に関する報告書を提供することによって，オペレータのシフト交替の間，処理の継続性を要求すること

13.6 運用ログ

コントロール目標

マネジメント･コントロールは，再構築，適時なレビュー，処理環境または処理支援などの他の活動の時系列的検証ができる十分な時系列的な情報が，運用ログの中に保管されていることが保証されること。

13.7 遠隔運用

コントロール目標

リモート運用について，遠隔サイトへのリンクの接続と切断に関する特定の手続が明示され，実施されることを保証すること。

M1

1 プロセスのモニタリング

1.1 モニタリングデータの収集

コントロール目標

ITと内部統制プロセスに関して，管理者は，内部と外部双方の情報源から関連する性能指標（例，ベンチマーク）が定義され，これらの諸指標に関連する管理情報報告書，例外報告書の作成にデータが収集されつつあることを保証すること。

1.2 パフォーマンスの評価

コントロール目標

情報サービス機能からデリバリされるサービスは，重要業績指標や重要成功要因で測定され，目標レベルと比較されること。評価は，継続的に情報サービス機能について実施されること。

1.3 顧客満足度の評価

コントロール目標

定期的な間隔で，管理者は，サービスレベルの不足を識別し，改善目的を設定するために，情報サービス機能によって提供されるサービスに関して，顧客満足度を測定すること。

1.4 管理者による報告

コントロール目標

マネジメント報告書は，組織の識別された進ちょく目標に対して，組織の上級管理者のレビュー用に提供されること。レビューによって，適切な管理者の行動が開始され，コントロールされること。

M2

2 内部統制の妥当性の評価

2.1 内部統制のモニタリング

コントロール目標

管理者は，管理者と監督者の行為，比較，照合調整とその他の日常的な行為を通じて，業務の通常のプロセスにおいて，内部統制の有効性をモニタリングすること。逸脱は，分析と修正行動が喚起されなければならない。

2.2 内部統制の適時な運用

コントロール目標

内部統制への信頼は，コントロールが迅速に目立ったエラーや不整合を目立たせ，これらが本番とデリバリに影響を与える前に是正されていることを要求する。エラー，不整合，例外に関する情報は，記録され，体系的に管理者に報告されること。

2.3 内部統制レベルの記録

コントロール目標

管理者は，内部統制システムの継続した有効性を保証するために，内部統制レベルと例外についての情報を，影響を受けるパーティに報告すること。意思決定の特定の階層で，どんな情報が必要とされるかを識別するために行動がとられること。

2.4 運用セキュリティと内部統制の保証

コントロール目標

運用セキュリティと内部統制の保証は，言明されたまたは含意されたセキュリティと内部統制要件に従ってセキュリティと内部統制が機能しているかどうかを確認するために，自己評価または独立した監査によって確立されること。管理者による継続したモニタリングは，脆弱性とセキュリティ問題を探すこと。

M3

3 独立した保証の確保

3.1 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

コントロール目標

管理者は，重要な新しいITサービスの導入に先立って，セキュリティと内部統制についての独立した認証／認定を得，そして，導入後の通常のサイクルに従って，それらのサービスについて，再認証／再認定を得ること。

3.2 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および内部統制の認証／認定

コントロール目標

管理者は，ITサービス･プロバイダの利用に先立って，セキュリティと内部統制についての独立した認証／認定を得，そして，通常のサイクルに従って，再認証／再認定を得ること。

3.3 ITサービスについての独立の有効性評価

コントロール目標

管理者は，ITサービスについて，通常のサイクルに従って，独立の有効性評価を得ること。

3.4 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

コントロール目標

管理者は，ITサービスプロバイダについて，通常のサイクルに従って，独立の有効性評価を得ること。

3.5 法律と規則の要件と契約上の誓約の独立の準拠性保証

コントロール目標

管理者は，通常のサイクルに従って，情報サービス機能における，法律と規則の要件および契約上の誓約事項についての準拠性の独立した保証を得ること。

3.6 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

コントロール目標

管理者は，通常のサイクルに従って，第三者機関のサービス･プロバイダにおける，法律と規則の要件および契約上の誓約事項についての準拠性の独立した保証を得ること。

3.7 独立保証機能の能力

コントロール目標

管理者は，独立保証機能が，そのようなレビューを効果的，効率的および経済的な方法で実施するのに必要な，技術上の競争力，およびスキルと知識を持つことを保証すること。

3.8 積極的な監査の関与

コントロール目標

IT管理者は，ITサービス･ソリューションの完了の前に，積極的な方法で，監査の関与を求めること。

M4

4 独立的監査の提供

4.1 監査規程

コントロール目標

監査機能の規程は，組織の上級経営者によって確立されること。この文書は，監査機能の責任，権限，説明責任の概要を述べること。規程は，監査機能の独立性，権限，説明責任が維持されていることを保証するために，定期的にレビューされること。

4.2 独立性

コントロール目標

監査人は，態度と外観において被監査部門から独立（実際および概念上も）していなければならない。監査人は，監査されている課や部門と関係があるべきでない。そして，可能な限り,対象組織自体からも独立していなければならない。このように,監査機能は,監査の客観的な完了を可能にっするために,監査対象領域から十分に独立していなければならない。

4.3 専門家としての倫理と基準

コントロール目標

監査機能は，適用可能な専門家の倫理規程（例　ISACA職業倫理基準）と彼らが行う全ての監査基準（例 ISACA情報システム監査基準）に準拠することを保証すること。職業上の注意義務は，適用可能な監査とIT基準の遵守を含む，監査業務のすべての面で実行されること。

4.4 能力

コントロール目標

管理者は，組織の情報サービス機能活動のレビューに責任を持つ監査人が，そのようなレビューを効果的，効率的および経済的な方法で実施するのに必要な，技術上の能力を持ち，集団としてスキルと知識（つまり，CISAドメイン）を持つことを，保証すること。管理者は，情報システム監査業務に配置された監査スタッフが，適切な職業上の継続教育を通じて，その技術上の能力を維持することを保証すること。

4.5 計画

コントロール目標

上級管理者は,定期的および独立した監査が，セキュリティと内部統制手続の有効性，効率性および経済性並びに情報サービス機能の活動をコントロールする管理者の能力についてなされていることを保証するために計画を策定すること。上級管理者は，この計画において，独立監査を得ることに関して優先順位を決定すること。監査人は，監査目標に取り組み，適用可能な職業監査基準を遵守するために，情報システム監査の作業を計画すること。

4.6 監査業務の実施

コントロール目標

監査人は，監査目標が達成され，そして，適用可能な職業監査基準に適合している保証を提供するために適切に監督されること。監査人は，監査目的を効率的に達成するために，十分で，信頼できる，適切な，そして有用な証拠を得ることを確保すること。監査の発見事項と結論は，適切な分析とこの証拠の解釈によって，支援されるべきである。

4.7 報告

コントロール目標

組織の監査機能は，監査作業の完了の上で意図している受領者に対し，適切な書式で報告書を提出する

こと。監査報告は,監査の範囲と目標，対象期間,実施した監査業務の性格と範囲を記述すべきである。報告書は，組織，意図している受領者，および，配付に関する制約について明示すること。監査報告書は，また，実施した監査業務に関する発見事項,結論および勧告並びに監査に関して監査人がもつ留保事項あるいは限定事項についても述べるべきである。

4.8 フォローアップ活動

コントロール目標

監査コメントの解決は，管理者による。監査人は，適切な行動が適時に行われたか否かを調べるために，以前の発見事項，結論，および，勧告に関する適切な情報を要求し，そして，評価すること。