

項目	リスク例	No	統制目標	統制の状況	関連文書	整備状況				運用状況					
						評価手続き	実施者	実施日	テスト結果	評価	評価手続き	実施者	実施日	テスト結果	評価
(1)開発・保守に関する手続の策定と保守	外部環境が変化したときに、開発やプログラムの変更管理、アクセス管理、運用にかかわる方針と手続が変更されないと、リスクが大きくなる。	1	企業はプログラム開発、プログラムの変更管理、プログラムやデータへのアクセス管理、コンピュータの運用に係る方針と手続が存在しており、経営者は適宜見直し、更新、承認する。	開発、変更管理等はソフトウェアの開発標準の手引きに方針が記載されており、変更が必要な場合は経営会議で見て直しが行われています。	・○○○規程 ・経営会議議事録	・○○○規程を入手し、財務報告に係るITに関連する方針と手続の変更に関する体制が整備されているか確認する。	内部監査人	20xx年 ○月○日	・○○○規程を入手し、財務報告に係るITに関連する方針と手続の変更に関する体制が整備されていることを確認した。	○	・○○○規程に基づいて、財務報告に係るITに関連する方針と手続が変更された際に、経営者や責任者がその変更を承認していることを確認する。	内部監査人	20xx年 ○月○日	・○○○規程に基づいて、財務報告に係るITに関連する方針と手続が変更された際に、経営者や責任者がその変更を承認していることを確認した。	○
	ITの開発の際に意図的な不正なプログラムが埋め込まれたり、処理の誤りが顕在化する。	1	ITを開発するための標準化された方針及び手続があり、これに基づいて、ITを開発し、更改する。	ソフトウェアの開発標準の手引きがあり、開発の際に意図的に不正なプログラムが埋め込まれることはありません。	・ソフトウェア開発手引書 ・業務分掌規程 ・職務権限規程 ・プロジェクト進捗表 ・プロジェクト会議議事録等	・ソフトウェア開発手引書を入手し、システム開発の標準的な手引きが整備されているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、システム開発の標準的な手引きが整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、システム開発が行われていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、システム開発が行われていることを確認した。	○
	ITの開発プロセスにおいて、意図的な不正や、処理に誤りの起きる可能性がある。	2	ITの開発プロセスにおいて、財務情報の信頼性に係る完全性、正確性、正当性の統制を確実に実現できるようにする。	ソフトウェア開発手引書に基づき、適切なIT業務処理の機能性が検討されており、入力桁数チェック等、不正が行われない仕組みが盛り込まれています。	・ソフトウェア開発手引書 ・システム要件定義書 ・概要書 ・仕様書等	・ソフトウェア開発手引書を入手し、誤りや不正を防止するための開発プロセスについて整備されているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、誤りや不正を防止するための開発プロセスについて整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、誤りや不正を防止するための開発が行われていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、誤りや不正を防止するための開発が行われていることを確認した。	○
		3	内部統制を意識した新規開発又はパッケージソフトの導入において、企画・開発・調達段階から検討し、文書化する。	ソフトウェア開発手引書に基づき、システムの要件定義書を作成する際にコントロールすべき項目について検討しております。		・ソフトウェア開発手引書を入手し、システムの要件定義書を作成する際にコントロールすべき項目について検討しております。	内部監査人	20xx年 ○月○日				内部監査人	20xx年 ○月○日		
		4	ITの開発では、財務情報の信頼性に係る統制機能をテストする。	ソフトウェア開発手引書に基づき、財務情報の信頼性に係る統制機能をテストしております。	・ソフトウェア開発手引書 ・統制機能テスト仕様書 ・統制機能テスト結果報告書等	・ソフトウェア開発手引書を入手し、財務情報の信頼性に係る統制機能のテストについて整備されているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、財務情報の信頼性に係る統制機能のテストについて整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、財務情報に係る過去のプロジェクトを調べ、テスト内容(二重売上等)を確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、財務情報に係る過去のプロジェクトを調べ、テスト内容(二重売上等)が適切であることを確認した。	○
	性能とキャパシティ不足によるシステムの利用ができない可能性がある。	5	性能とキャパシティに関する計画は、システム設計と導入活動に含まれている。	ソフトウェア開発手引書に基づき、システムの要件定義書作成時には、サーバ、アプリ、ネットワーク、それぞれに関する性能と将来的な必要キャパシティ(CPU、メモリ、HDD等)について記載し、システム設計書にも同様の内容が反映されております。	・ソフトウェア開発手引書 ・システム要件定義書 ・システム設計書 ・システム構成図 ・ハード・ソフトウェア一覧	・ソフトウェア開発手引書を入手し、性能とキャパシティに関する計画について整備されているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、性能とキャパシティに関する計画について整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、性能、キャパシティを検討し、要件定義書を作成したことを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、性能、キャパシティを検討し、適切に要件定義書が作成されていることを確認した。	○
本番環境にプログラムを移行する際にプログラムが改ざんされる。	6	プログラムの本番移行に際して、移行を責任者が承認し、移行作業にあたっては権限の分離を行う。	本番移行時の手続は作業担当の分離を含めてシステム運用手引書に定められており、しかるべき役割の承認がないと移行できないようになっています。	・システム設計書 ・ソフトウェア開発手引書 ・組織図	・ソフトウェア開発手引書を入手し、プログラムの移行手順・体制が整備されていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、プログラムの移行手順・体制が整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、プログラムの移行が行われていることを確認する。 ・変更作業の担当、承認担当等、職務の分離が行われているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、プログラムの移行が行われていることを確認した。 ・変更作業の担当、承認担当等、職務の分離が行われていることを確認した。	○	
(3)IT基盤の構築	IT基盤のインターフェースが正常に機能しない為、扱うデータの信頼性が確保できない。	1	転送されたデータが信頼できることを確かめるために、IT基盤のインターフェースのテストを実施する。	ソフトウェア開発手引書に基づいて、インターフェーステストを実施し、データ検証しております。	・ソフトウェア開発手引書 ・システム要件定義書 ・システム構成図 ・システム設計書 ・操作・設定手順書 ・インターフェース仕様書 ・システム連携仕様書 ・インターフェーステスト仕様書 ・インターフェーステスト結果報告書等	・ソフトウェア開発手引書を入手し、IT基盤のインターフェースの操作手順・設定基準が整備されているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、IT基盤のインターフェースの操作手順・設定基準が整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、インターフェーステストを実施し、データの正確性を検証したことを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、インターフェーステストを実施し、データの正確性を検証したことを確認した。	○
	IT基盤の設定が不適切な場合、システムが正しく動作しない。	2	IT基盤の設定を適切に維持し、認識外の変更は抑制する。	構成管理マニュアルに基づいて、ネットワーク、PC、ソフトの構成管理を行っており、操作ログを定期的に検証しております。	・構成管理マニュアル ・PC利用マニュアル ・操作・設定手順書 ・操作ログ一覧表	・構成管理マニュアルを入手し、IT基盤の手順・設定、維持される仕組みが整備されているか確認する。	内部監査人	20xx年 ○月○日	・構成管理マニュアルを入手し、IT基盤の手順・設定、維持される仕組みが整備されていることを確認した。	○	・構成管理マニュアルに基づいて、変更が行われた場合のログ等が記載された資料を確認する。	内部監査人	20xx年 ○月○日	・構成管理マニュアルに基づいて、変更が行われた場合のログ等が記載された資料を確認した。	○
(4)変更管理	プログラムが改ざんされたり、承認なく変更される。	1	システムソフトの変更を含むプログラム変更、システムの変更及び保守管理の文書化を行い、記録、承認等、変更管理手続に従うようにする。	システム設計書、システム運用手引書に基づいて、変更管理手続を行っております。	・ソフトウェア開発手引書 ・変更手順書 ・システム設計書 ・変更申請書 ・変更結果報告書	・ソフトウェア開発手引書を入手し、変更管理の手順・体制が整備されていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、変更管理の手順・体制が整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、プログラムの変更が行われていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、プログラムの変更が行われていることを確認した。	○
	緊急時にプログラムが改ざんされたり、承認なく変更される。	2	緊急の変更依頼は文書化された正式な変更管理手続に従うようにする。	システム設計書、システム運用手引書に緊急の変更依頼についても記載されており、取り消しの手順も含めて標準化され、しかるべき役割の承認が行うようになっております。	・システム設計書 ・ソフトウェア開発手引書 ・変更手順書 ・緊急変更結果報告書	・ソフトウェア開発手引書を入手し、緊急時の変更管理の手順・体制が整備されていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、緊急時の変更管理の手順・体制が整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、緊急時のプログラム変更が行われていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、緊急時のプログラム変更が行われていることを確認した。	○
	本番環境に変更結果を移行する際にプログラムが改ざんされる。	3	変更されたプログラムの本番移行に際して、移行を責任者が承認し、移行作業にあたっては権限の分離を行う。	本番移行時の手続は作業担当の分離を含めてシステム運用手引書に定められており、しかるべき役割の承認がないと移行できないようになっています。	・ソフトウェア開発手引書 ・システム設計書 ・組織図	・ソフトウェア開発手引書を入手し、変更されたプログラムの移行手順・体制が整備されていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、変更されたプログラムの移行手順・体制が整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、変更されたプログラムの移行が行われていることを確認する。 ・変更作業の担当、承認担当等、職務の分離が行われているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、変更されたプログラムの移行が行われていることを確認した。 ・変更作業の担当、承認担当等、職務の分離が行われていることを確認した。	○
テストが事前に計画されていないとテスト項目に漏れが起きる。	1	IT基盤のテスト計画を事前に関係者でチェックして、テスト内容やテスト項目に漏れがないようする。	ソフトウェア開発手引書に基づいて、テスト仕様書を作成する際、IT部門だけでなく、利用する部門も打合せを行い、テスト項目の洗い出し、実施方法を検討しております。	・ソフトウェア開発手引書 ・関連部門会議議事録 ・テスト仕様書 ・テスト実施手順書	・ソフトウェア開発手引書を入手し、テスト実施時の計画・打ち合わせを行う体制が整備されているか確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、テスト実施時の計画・打ち合わせを行う体制が整備されていることを確認した。	○	・ソフトウェア開発手引書に基づいて、テストの内容や計画が事前に関係者に照会され、承認されていることを確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、テストの内容や計画が事前に関係者に照会され、承認されていることを確認した。	○	

① 情報システムのソフトウェア開発・調達

項目	リスク例	No	統制目標	統制の状況	関連文書	整備状況				運用状況				
						評価手続き	実施者	実施日	テスト結果	評価	評価手続き	実施者	実施日	テスト結果
(5)テスト	テストが不十分なため、不完全なプログラムが本番環境で稼働し、業務要件を満足できない危険性がある。	2	IT基盤の機能が正しく動作するかを検証するために、単体テスト、システムテスト、統合テスト、受入テストを実施する。	ソフトウェア開発手引書に基づいて、テスト仕様書を作成し、単体テスト、システムテスト、受け入れテストを実施しております。	・ソフトウェア開発手引書 ・テスト実施手順書 ・システム設計書 ・インタフェース仕様書 ・システム連携仕様書 ・単体テスト仕様書 ・結合テスト仕様書 ・受け入れテスト仕様書 ・テスト結果報告書等	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、各工程のテストの実施について手順・体制が整備されているか確認する。	○	・ソフトウェア開発手引書に基づいて、テストが実施されている事を確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、テストが実施されていることを確認した。	○
		3	IT基盤の更改では、アプリケーション・システム等のマスターデータの配信、新旧システム間でのデータ変換、データ転送、財務情報の配信等のテストを実施する。	ソフトウェア開発手引書に基づいて、テスト仕様書を作成し、マスターデータ移行テスト等を実施しております。	・ソフトウェア開発手引書 ・システム設計書 ・テスト実施手順書 ・インタフェース仕様書 ・システム連携仕様書 ・移行テスト仕様書 ・テスト結果報告書等	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、各工程のテストの実施について手順・体制が整備されているか確認する。	○	・ソフトウェア開発手引書に基づいて、テストが実施されている事を確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、テストが実施されていることを確認した。	○
		4	テスト計画と確立されたテスト標準に従って、ロードテスト(負荷テスト)や限界性能テストを実施する。	ソフトウェア開発手引書に基づいて、テスト仕様書を作成し、運用時のデータ量を想定した負荷テスト及び限界性能を確認するためのテストを実施しております。	・ソフトウェア開発手引書 ・システム設計書 ・テスト実施手順書 ・インタフェース仕様書 ・システム連携仕様書 ・負荷テスト仕様書 ・限界性能テスト仕様書 ・テスト結果報告書等	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、ピーク負荷による性能低下の有無、限界性能テストの実施について手順・体制が整備されているか確認する。	○	・ソフトウェア開発手引書に基づいて、負荷テスト・限界性能テストが実施されている事を確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、負荷テスト・限界性能テストが実施されていることを確認した。	○
	財務情報データを旧システムから新システムに移行する際に、テストが行われず、移行したデータが正確かどうか判断できない。	5	新システムに移行されたデータが信頼できることを確認するため、旧システムのデータ統合テストを実施する。	ソフトウェア開発手引書に基づいて、テスト仕様書を作成し、本番移行検証を行い、データに差異がないことを確認しております。	・ソフトウェア開発手引書 ・システム設計書 ・インタフェース仕様書 ・システム連携仕様書	内部監査人	20xx年 ○月○日	・財務情報のデータ移行が実施された際の内容(データの突合、差異リスト、追加機能、DBの項目のテスト、受入テストの有無等)と結果を調べ、データの移行の責任者及び受け入れ側の承認について確認する。	○	整備状況評価と同様の手続となる。	内部監査人	20xx年 ○月○日	整備状況評価と同様の手続となる。	○
	受入テストをシステム開発した担当者が実施すると、誤りや不正が見逃される可能性がある。	6	財務情報に係る情報システムの受入テストでは、ユーザ部門等、開発担当者以外の者を参照させる。	ソフトウェア開発手引書に基づいて、テスト仕様書を作成し、開発担当者以外のテスト要員によるテスト及び、利用部門によるテストを実施しております。	・ソフトウェア開発手引書 ・受入テストユーザマニュアル ・受入テスト仕様書 ・受入テスト結果報告書等	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書を入手し、ユーザーによる受入テストの実施について手順・体制が整備されているか確認する。	○	・ソフトウェア開発手引書に基づいて、ユーザーによる受入テストが実施されている事を確認する。	内部監査人	20xx年 ○月○日	・ソフトウェア開発手引書に基づいて、ユーザーによる受入テストが実施されていることを確認した。	○
	テスト結果の記録が残されていないと、機能が正しく開発されているかの証拠がない。	7	財務情報に係る情報システムの重要なテスト(受入テスト等)では、テスト項目や結果を記録して、保管する。	ソフトウェア開発手引書に基づいて、重要な項目以外も全てテストを行っており、結果を保管しております。	・ソフトウェア開発手引書	内部監査人	20xx年 ○月○日	・財務に係るシステムで過去のプロジェクトから、重要なテストについて、実施の有無が記録・保管されていることを確認する。	○	整備状況評価と同様の手続となる。	内部監査人	20xx年 ○月○日	整備状況評価と同様の手続となる。	○
	(1)運用管理	運用時の誤操作によって誤った処理が行われる。	1	システムを運用するための標準化された方針及び手続があり、これに基づいて、運用する。	システム運用手引書に基づいて業務が行われており、適切な権限保有者が承認を行っております。	・システム運用手引書 ・業務分掌規程 ・職務権限規程 ・プロジェクト進捗表 ・プロジェクト会議議事録等	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、システム運用の標準的な手引きが整備されているか確認する。	○	・システム運用手引書に基づいて、運用業務が行われている事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、運用業務が行われていることを確認した。
バッチジョブに関する運用手順が明確でない、またはマニュアルの内容に問題があることなどによって、適切・確実なジョブ運用が保証されない。		2	ジョブスケジュールの登録・変更・臨時ジョブの実行・ジョブ異常時の対応方法に関する運用マニュアルが構築され、適切な権限保有者が承認している。	システム運用手引書に基づいて、ジョブが適切に運用されており、適切な権限保有者が承認を行っております。	・システム運用手引書 ・ジョブ設定手順書 ・ジョブ一覧 ・臨時ジョブ申請書 ・異常ジョブ対応結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、ジョブの運用・設定・手順・体制、また臨時ジョブ・ジョブ異常発生時の対応方法が整備されているか確認する。	○	・システム運用手引書に基づいて、ジョブスケジュール通りに運用されているか確認する。自動化されている場合は、ジョブスケジュールを変更できない仕組み(アクセス制限や丹生退出管理)がある事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、ジョブスケジュール通りに運用されていることを確認した。自動化されている場合は、ジョブスケジュールを変更できない仕組み(アクセス制限や丹生退出管理)があることを確認した。	○
運用時の不正な操作等を発見できない。		3	情報システムとデータ処理について、企業にログ採取・分析についての方針があり、それに基づいてログが採取されて、必要な項目をモニタリングする。	システム運用手引書に基づいて、ログ採取・分析に必要な項目を定期的にモニタリングしております。	・システム運用手引書 ・ログ手順書 ・ログ検証結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、ログ採取・分析に関する手順・体制が整備されているか確認する。	○	・システム運用手引書に基づいて、ログを採取し、不正操作等のモニタリングに必要な項目を定期的にモニタリングされているか確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、ログを採取し、不正操作等のモニタリングに必要な項目を定期的にモニタリングされていることを確認した。	○
情報システムが処理するデータの信頼性が保証されない。		4	情報システムとデータ処理のログが取得され、ログファイルの完全性、正確性、正当性を保証する仕組み(改ざんされないログが記録され、保管されている)を構築する。	システム運用手引書に基づいて、信頼性を担保出来るログツールを使用し、運用ログを取得している。	・システム運用手引書 ・ログ手順書 ・ログツール設計書 ・ローグ一覧表	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、ログの記録や保管に際しての手順・体制が整備されているか確認する。	○	・システム運用手引書に基づいて、適切にログを記録・保管している事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、適切にログを記録・保管していることを確認した。	○
		5	不十分な性能とキャパシティに適切対応する仕組みがあり、キャパシティ不足によるログの取得漏れがないようにする。	システム運用手引書に基づいて、性能劣化やディスクの容量不足に対して閾値の設置、その値を超えた場合の管理者への通知機能を設定している。	・システム運用手引書 ・性能・キャパシティ設定手順 ・通知報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、サーバー、ネットワークの性能劣化、ディスク容量の不足に対するマニュアルが整備されているか確認する。	○	・システム運用手引書に基づいて、サーバー、ネットワークの性能劣化、ディスク容量の不足に対応している事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、サーバー、ネットワークの性能劣化、ディスク容量の不足に対応していることを確認した。	○
財務情報に係る情報システムの担当者が、リスクと適切な操作方法等について教育を受けていないと、誤操作によるシステムの誤りや不正の防止につながる。		6	財務情報に係る情報システムが新しく導入される際には、担当者に適切な教育が計画され、実施する。	中期事業計画書・人材育成マニュアルに基づいて、システムの導入時には計画に基づき実施されており、合わせて人員への教育も行っております。	・中期事業計画書 ・人材育成マニュアル ・セミナーテキスト ・カリキュラムスケジュール ・セミナー対象者名簿	内部監査人	20xx年 ○月○日	・中期事業計画書・人材育成マニュアルを入手し、担当者への教育体制が整備されているか確認する。	○	・中期事業計画書・人材育成マニュアルに基づいて、カリキュラムとスケジュール、受講者を確認し、担当者の教育が適切に行われている事を確認する。	内部監査人	20xx年 ○月○日	・中期事業計画書・人材育成マニュアルに基づいて、カリキュラムとスケジュール、受講者を確認し、担当者の教育が適切に行われていることを確認した。	○
②情報システムの		ソフトウェア、ハードウェア、アプリケーション・システム等が無断で設置・廃棄されることにより、誤処理やシステム停止が起こる。	1	企業において使用されるソフトウェア等に関して、無許可のソフトウェアの発見・防止が適切に行われている。	情報システムの購入から廃棄までの手続きが定められており、購入済みの資産は定期的に現品確認を行い、管理外の機器が存在しないか確認しております。又、定期的にPCの構成ログを採取し、無許可のソフトウェアがあれば削除しております。	・構成管理マニュアル ・現品棚卸一覧表 ・構成ローグ一覧表 ・構成管理台帳 ・固定資産台帳	内部監査人	20xx年 ○月○日	・構成管理マニュアルを入手し、情報システムの購入から廃棄までの手順・体制が整備されているか確認する。	○	・構成管理マニュアルに基づいて、現品確認の実施や構成ログの採取等を行い、情報システムが構成管理台帳と固定資産管理に正しく反映されている事を確認する。	内部監査人	20xx年 ○月○日	・構成管理マニュアルに基づいて、現品確認の実施や構成ログの採取等を行い、情報システムが構成管理台帳と固定資産管理に正しく反映されていることを確認した。
	変更が正しくシステム管理情報に反映されないために、システムの不整合が起きるリスクがある。	2	変更管理の結果を適時、構成管理に反映する。	システム運用手引書に変更管理についても記載されており、それに基づいて機器の変更やマスタの変更を行った際、管理台帳に記録しております。	・構成管理マニュアル ・システム運用手引書 ・構成管理台帳 ・変更結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、構成の変更管理について整備されているか確認する。	○	・システム運用手引書に基づいて、機器やマスタ等の変更管理の結果を構成管理台帳に正しく反映されている事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、機器やマスタ等の変更管理の結果を構成管理台帳に正しく反映されていることを確認した。	○

項目	リスク例	No	統制目標	統制の状況	関連文書	整備状況				運用状況				
						評価手続き	実施者	実施日	テスト結果	評価	評価手続き	実施者	実施日	テスト結果
(2)構成管理	管理期限の経過したハードウェア等の継続使用により、処理に誤りが起こるリスクがある。	3	情報資産の有効期限を適切に管理し、更新する。	ハード、ソフト共に有効期限があるもの(リースや年度契約製品)は管理台帳により事前に知ることができ、次の手続きを行えるようになっております。	・構成管理マニュアル ・構成管理台帳 ・固定資産台帳	内部監査人	20xx年 ○月○日	・構成管理マニュアルを入手し、情報資産の管理について整備されているか確認する。	○	・構成管理マニュアルに基づいて、情報資産の有効期限が正しく記録され、期限に合わせて使用停止等が構成管理台帳で管理されている事を確認する。	内部監査人	20xx年 ○月○日	・構成管理マニュアルに基づいて、情報資産の有効期限が正しく記録され、期限に合わせて使用停止等が構成管理台帳で管理されていることを確認した。	○
	ソフトウェアとネットワーク基盤が適切に設定されておらず、誤処理やシステム停止が発生する。	4	ソフトウェアとネットワーク基盤が適切に設定されていることを確認するため、定期的にテストと評価を実施している。	情報システム部門は、情報セキュリティ規程に基づいて、定期的にテストデータを流し設定の適切性を確認しております。	・情報セキュリティ規程 ・構成管理マニュアル ・テスト仕様書 ・テスト結果報告書	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、ネットワーク基盤の設定・テスト手順や体制が整備されていることを確認する。	○	・情報セキュリティ規程に基づいて、ソフトウェアとネットワーク基盤の設定の適切性テストを行っている事を確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、ソフトウェアとネットワーク基盤の設定の適切性テストを行っていることを確認した。	○
	出力データの配送や保存について手続が定められていないと財務情報が紛失したり、伝達できなくなる。	1	財務情報が適切に処理され、然るべき権限者に適時に伝達される手続が確立されており、これに従うようにする。	各部門に業務マニュアルを完備しており、出力したデータが正しい受取人に配送されるようになっております。	・各種業務マニュアル ・証憑	内部監査人	20xx年 ○月○日	・各種業務マニュアルを入手し、処理データ及び報告用出力の取扱い、配布、保存に関する手続が整備されているか確認する。	○	・各種業務マニュアルに基づき、処理データ及び報告用出力の取扱い、配布・保存が実施され、誤送等がない事を確認する。	内部監査人	20xx年 ○月○日	・各種業務マニュアルに基づき、処理データ及び報告用出力の取扱い、配布・保存が実施され、誤送等がないことを確認した。	○
	データの保管や移送の際には、改ざん、不正複写等の可能性がある。	2	財務情報の保管及び移送に際して、不正アクセス、改ざんから保護する仕組みを構築する。	情報セキュリティ規程に基づいて、適切なアクセス権が設けられており、保管場所の入退室管理が実施されています。	・情報セキュリティ規程 ・入退室管理台帳	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、財務情報の保管及び移送に関して、手順が整備されているか確認する。	○	・情報セキュリティ規程に基づいて、情報セキュリティ対策(施設等)が実施されている事を、又、入退室管理等の物理的セキュリティ対策が実施されている事を確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、情報セキュリティ対策(施設等)が実施されていること、又、入退室管理等の物理的セキュリティ対策が実施されていることを確認した。	○
	文書やデータについては、保管が正しくなれず、重要な情報を紛失したり、無駄なデータが長期保管される。	3	文書類、データの保管期間と条件を定める。	文書管理規定に基づいて、情報の種類(設計図、経理データ等)により保管期間を設け、その期間に従って保管するようしております。	・情報セキュリティ規程 ・文書管理規程 ・保管文書一覧表	内部監査人	20xx年 ○月○日	・文書管理規程・情報セキュリティ規程を入手し、書類やデータ報告書等の保管期間と条件が整備されているか確認する。	○	・文書管理規程・セキュリティ管理規程に基づいて、適切な保管が実施されている事を確認する。	内部監査人	20xx年 ○月○日	・文書管理規程・セキュリティ管理規程に基づいて、適切な保管が実施されていることを確認した。	○
	電子データの復旧は定期的にテストが行われている。	4	電子データの復旧は定期的にテストが行われている。	情報セキュリティ規程に基づいて、年に1回、復旧訓練を行っております。	・情報セキュリティ規程	内部監査人	20xx年 ○月○日	・電子データの復旧について、記載された文書を確認し、また訓練記録などで、実施の確認をする。	○	整備状況評価と同様の手続となる。	内部監査人	20xx年 ○月○日	整備状況評価と同様の手続となる。	○
(3)データ管理	バックアップされていないと、データを消失した場合に、復元ができない。	5	データやプログラムのバックアップ・リカバリに関する手順が策定されている。	システム運用手引書には、データ及びプログラムのリカバリ手順が記載されており、それに基づいて破損したシステムやディスク、データベースなどを復旧することとなっております。	・システム運用手引書 ・リカバリ手順書 ・リカバリ結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、データとプログラムをリカバリするための方針と手順が整備されているか確認する。	○	・システム運用手引書に基づいて、修復が適切に行われている事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、修復が適切に行われていることを確認した。	○
		6	システム運用手引書に基づき、データ及びプログラムのバックアップは定期的に実施しており、外部倉庫にバックアップ媒体を保管しております。	システム運用手引書に基づき、データ及びプログラムのバックアップは定期的に実施しており、外部倉庫にバックアップ媒体を保管しております。	・システム運用手引書 ・バックアップ手順書 ・バックアップ結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、データとプログラムをバックアップするための方針と手順が整備されているか確認する。	○	・システム運用手引書に基づいて、バックアップが適切に行われ、保管場所、保管状況が正しいか確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、バックアップが適切に行われ、保管場所、保管状況が正しいことを確認した。	○
(1)情報セキュリティフレームワーク	情報セキュリティの基本指針とフレームワークがなければ、情報システムにおけるアクセス管理が適切に実施されない。	1	情報セキュリティのフレームワーク(情報セキュリティ基本方針、対策基準などを)を構築する。	情報セキュリティに関する基本方針は情報セキュリティ規程に記載されており、その内容は定期的に情報システム委員会で見直しが行われております。	・情報セキュリティ規程 ・組織図 ・業務分掌規程 ・職務権限規程 ・プロジェクト進捗表 ・プロジェクト会議議事録等	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、情報セキュリティの標準的な手引きが整備されているか確認する。	○	・情報セキュリティ規程に基づいて、セキュリティのフレームワークが現場で機能し、維持する体制がある事を確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、セキュリティのフレームワークが現場で機能しており、維持する体制があることを確認した。	○
③内外からのアクセス管理等のシステムの安全性の確保	適切な認証がないと、データへの改ざんや不正な参照が起きる。	1	すべての担当者の認証及びアクセス制御機能が存在し、アクセスログを記録する。	情報セキュリティ規程でアクセス権について明記されており、それに基づき利用者の権限を設定しております。利用に関してはログインパスワードの制御を行っており、ログイン後は無操作時間が一定時間に達すると画面がロックするようになっております。又、アクセスログは自動で取得され、サーバーで一元管理しております。	・情報セキュリティ規程 ・アクセス管理規程 ・アクセス権一覧表 ・アクセスログ一覧表	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、管理者、担当者に対する認証及びアクセス制御に関する手順・体制が整備されているか確認する。	○	・情報セキュリティ規程に基づいて、管理者、担当者に対する認証及びアクセス制御を行い、アクセスログを採取している事を確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、管理者、担当者に対する認証及びアクセス制御を行い、アクセスログを採取していることを確認した。	○
	担当者のアカウントの発行、停止等の管理がなされていないと不正使用されて、データへの改ざんや漏えいが発生する。	2	認証及びアクセス制限の有効性を保つために方針・手続が存在し、適切に運用されている。	アカウントの申請～廃止までの手続はマニュアルに記載されており、それに基づき適時処理を行っております。	・アクセス管理規程 ・アカウント発行手順書 ・アカウント申請～廃止申請書 ・人事異動、入退社記録	内部監査人	20xx年 ○月○日	・アクセス管理規程を入手し、アカウントの申請～廃止の手順・体制が整備されているか確認する。	○	・アクセス管理規程に基づいて、利用者の登録、変更及び削除の手続の実施、変更毎に処理(特に退職時)されている事を確認する。	内部監査人	20xx年 ○月○日	・アクセス管理規程に基づいて、利用者の登録、変更及び削除の手続の実施、変更毎に処理(特に退職時)されていることを確認した。	○
	担当者のアカウントの申請、設定、発行、一時停止、廃止に関する手続が確立し、手順に従って適時に処理する。	3	担当者のアカウントの申請、設定、発行、一時停止、廃止に関する手続が確立し、手順に従って適時に処理する。	担当者のアカウントの申請、設定、発行、一時停止、廃止に関する手続が確立し、手順に従って適時に処理する。		内部監査人	20xx年 ○月○日				内部監査人	20xx年 ○月○日		
	適切なアクセス制御機能がなく、データへの改ざんや不正な参照が起きる。	4	アクセス権に関して、適宜見直し・確認のための統制プロセスを構築し、これに従う。	アクセス権は定期的に見直ししており、見直しのタイミングでアクセスログの検証も行っております。	・情報セキュリティ規程 ・職務権限規程 ・人事異動、入退社記録 ・アクセス権一覧表 ・アクセスログ	内部監査人	20xx年 ○月○日	・セキュリティ管理規程を入手し、アクセス権について手順・体制が整備されているか確認する。	○	・セキュリティ管理規程に基づいて、異動等があった場合等、アクセス権が職務権限と一致しているか、又、適宜アカウントを見直している事を確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、異動等があった場合等、アクセス権が職務権限と一致しているか、又、適宜アカウントを見直していることを確認した。	○
	インターネットを利用する場合は不正侵入等の脅威がある。	5	電子商取引等にインターネット等外部のネットワークを利用する場合は、ファイアウォール、侵入検知システム等が用いられている。さらに、脆弱性評価の結果によるパッチ適用等の適切な統制を構築し、不正アクセスを防ぐ。	外部への接続はファイアウォール経由で行っており、全てのPOCにはウイルスチェックのソフトウェアがインストールされ、適時パターンファイルのアップデートを行っております。	・情報セキュリティ規程 ・ネットワーク設定手順書 ・脆弱性評価結果報告書 ・対策システム導入会議議事録 ・構成管理台帳 ・構成管理台帳	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、外部からの不正侵入に対する対策手順・体制が整備されているか確認する。	○	・情報セキュリティ規程に基づいて、ファイアウォールや侵入検知システムを含む外部からのアクセス制御が実施され適切であること、又、ウイルス防止システムが、財務情報に係るシステムのセキュリティを保護するために用いられている事を確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、ファイアウォールや侵入検知システムを含む外部からのアクセス制御が実施され適切であること、又、ウイルス防止システムが、財務情報に係るシステムのセキュリティを保護するために用いられていることを確認した。	○
	職務権限が決まられていないと、不正なアクセスが起きて、データが改ざんされる危険性がある。	6	システムとデータへのアクセス権の申請と承認に関して、職務分離をする。	システム管理者と通常運用でデータをアクセスする人員は別々にしており、同一人物で両方の操作はできないようになっております。	・情報セキュリティ規程 ・システム運用手引書 ・職務権限規程 ・ID棚卸表	内部監査人	20xx年 ○月○日	・職務権限規程を入手し、適切に権限が付与され、運用されているか確認する。	○	・職務権限規程に基づいて、適切にアクセス権が付与されている事を確認する。	内部監査人	20xx年 ○月○日	・職務権限規程に基づいて、適切にアクセス権が付与されていることを確認した。	○
	特権ユーザは情報システムの変更や担当者の追加・削除等ができるため、統制されない改ざん等の不正が発生する。	7	特権については運用基準があり、特権の付与に際して最小限にとどめ、利用終了後は速やかに特権を停止する。	本番環境においては一般利用者には特権の付与を行っておりませんので、問題ありません。	・情報セキュリティ規程 ・システム運用手引書 ・職務権限規程 ・アカウント設定基準 ・ID棚卸表	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、特権IDの運用・付与基準が整備されている事を確認する。	○	・システム運用手引書に基づいて、特権IDを調査し、正しい職務に適切に付与されている事を確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、特権IDを調査し、正しい職務に適切に付与されていることを確認した。	○

項目	リスク例	No	統制目標	統制の状況	関連文書	整備状況				運用状況				
						評価手続き		実施者	実施日	テスト結果		評価	評価手続き	
(3)情報セキュリティインシデントの管理	施設へのアクセスに制限がなければ、関係者でない人物によって重要な財務情報にアクセスされたり、改ざんされたりする。	8	施設へのアクセスは権限のある者に制限され、適切なIDの付与と認証を実施する。	サーバーールームや重要書類が保管されている場所への入室は専用のIDカードがないと入れないようになり、IDカードの利用ログも取得されるようになっております。	・情報セキュリティ規程 ・情報セキュリティ規程 ・入室記録	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、サーバーールーム・重要書類保管場所への入室に関する方針や手続・体制が整備されていることを確認する。	○	・情報セキュリティ規程に基づいて、入室に関する記録を取得し、定期的に検査されていることを確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、入室に関する記録を取得し、定期的に検査されていることを確認した。	○
	情報セキュリティインシデントへの対応が適切に行われず、被害が拡大する。	1	情報セキュリティインシデントが発生したとき、適時に記録・分析・解決をする。	情報セキュリティに関する問題が発生した場合は、情報セキュリティ規程に則り、適時に対応が行われ、内容を分析し、次回から発生しないような対策を講じております。	・情報セキュリティ規程 ・障害対応手順書 ・セキュリティインシデント一覧 ・インシデント対応報告書	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、セキュリティインシデントの対応方法・手順が整備されていることを確認する。	○	・情報セキュリティ規程に基づいて、セキュリティインシデントの報告書等の有無を確認し、インシデントが適時に対応(記録、分析又は解決)されていることを確認する。	内部監査人	20xx年 ○月○日	・情報セキュリティ規程に基づいて、セキュリティインシデントの報告書等の有無を確認し、インシデントが適時に対応(記録、分析又は解決)されていることを確認した。	○
	ログ取得されず、インシデントの原因究明ができない。	2	適切なログ管理機能が存在し、インシデントの原因を究明する仕組みを構築する。(同じインシデントの再発のリスクの低減などの仕組み)	ログ管理ツールを導入しており、ログからインシデント原因を究明出来る機能が整備されております。	・情報セキュリティ規程 ・情報セキュリティインシデント一覧報告書	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、インシデントの対応・手順・再発防止策等が整備されていることを確認する。	○	・ログ情報を入手し、インシデントの対応を行ったことを確認する。	内部監査人	20xx年 ○月○日	・ログ情報を入手し、インシデントの対応を行ったことを確認した。	○
	承認されていない行為をモニタリングできず不正な行為が行われて、インシデントが発生する。	3	不正行為等が起きた場合に、適時に管理者に通知し、警告する機能(ユーザアカウントをロックする等)、セキュリティインシデント対応の機能を整備する。	不正アクセスが発生した際、管理者に通知される仕組みがあり、即時対応できる体制が整っております。	・情報セキュリティ規程 ・障害対応手順書 ・不正アクセス通知書	内部監査人	20xx年 ○月○日	・情報セキュリティ規程を入手し、不正行為が発生した際、直ちに検知し、対応できる手順・対応が整備されていることを確認する。	○	・情報セキュリティ規程に基づいて、不正アクセスが発生した際に、漏れなく検知・対応し、適切に管理者へ報告されていることを確認する。	内部監査人	20xx年 ○月○日	・不正アクセス通知書を入力し、漏れなく検知・対応し、適切に管理者へ報告されていることを確認した。	○
(1)委託先との契約	委託先選定基準が不明確で、不適格な業者を選定すると、サービス品質が低くなり、納期が守れなかったりして、財務情報の信頼性を保証できなくなる。	1	委託先の選定前に、責任者が候補業者のサービス提供能力の評価と財務上の持続性に関して、適格性を判断する。	委託外注管理規程に基づいて、委託先は複数の業者から、もっとも評価が高い業者を選定するように記載されており、事前に実績やサービスレベル等を確認しております。	・委託外注管理規程 ・外注先選考資料	内部監査人	20xx年 ○月○日	・委託外注管理規程に委託先の財務上の安定性、財務情報に係るIT統制に関する経験や知識(過去の類似案件の件数、資格者の数等)が含まれていることを確認する。	○	・委託外注管理規程に基づいて、委託先は複数の業者から、もっとも評価が高い業者が選定され、事前に実績やサービスレベル等を確認していることを確認する。	内部監査人	20xx年 ○月○日	・委託外注管理規程に基づいて、委託先は複数の業者から、もっとも評価が高い業者が選定され、事前に実績やサービスレベル等を確認していることを確認した。	○
	委託先選定や委託先の管理方針が不明確であると、サービスレベルが維持できなくなり、委託した財務情報が適切に得られなくなる。	2	開発業務、運用業務、物流・保管業務等、用途に応じた委託先選定方針に沿って委託先を選定する。	委託外注管理規程に基づいて、業者を選定しております。	・委託外注管理規程 ・委託先選定方針 ・委託先選定結果書	内部監査人	20xx年 ○月○日	・委託外注管理規程を入手し、委託先の選定や管理、方針が整備されていることを確認する。	○	・委託外注管理規程に基づいて、委託先の選定や管理が適切に行われていることを確認する。	内部監査人	20xx年 ○月○日	・委託外注管理規程に基づいて、委託先の選定や管理が適切に行われていることを確認した。	○
	委託先とのサービスレベルの契約がセキュリティ統制について触れていないと、サービスレベルが維持できなくなり、適切に財務情報が作成されなくなる。	3	業務の委託前に委託先との契約について社内承認され、契約書が交わされるための手続(内部統制の要件定義と委託先の受諾条件が含まれる)があり、これに従うようにする。	委託外注管理規程に基づいて、事前に契約内容を社内で協議しており、委託先が当社の情報セキュリティの基準に準拠しているかを確認しております。	・委託外注管理規程 ・委託先選定会議議事録 ・SLA ・契約書サンプル	内部監査人	20xx年 ○月○日	・委託外注管理規程を入手し、契約に関する社内協議の実施、手順・体制が整備されていることを確認する。	○	・契約時に社内の然るべき役職の承認を得ていることを確認する。	内部監査人	20xx年 ○月○日	・契約時に社内の然るべき役職の承認を得ていることを確認した。	○
	委託先とのサービスレベルの内容を見直さないと、サービス品質が低下しても分からない。	4	委託先の信頼性(完全性、正確性、正当性)のサービスレベル、内部統制状況について調査する。	委託外注管理規程に基づいて、事前の調査では委託先の内部統制の状況確認をチェックシートを用いて行っており、契約後の品質も定期的に評価しております。	・委託外注管理規程 ・SLA ・品質チェックシート ・内部統制報告書	内部監査人	20xx年 ○月○日	・委託外注管理規程に、定期的なサービスレベル、内部統制状況の確認に関する記載があることを確認する。	○	・定期的なサービスレベル、内部統制状況の確認を行っていることを確認する。	内部監査人	20xx年 ○月○日	・定期的なサービスレベル、内部統制状況の確認を行っていることを確認した。	○
(2)委託先とのサービスレベルの定義と管理	サービスレベルが定義されていないと、安定したサービスを継続して利用できず、財務情報の信頼性が損なわれる。	1	財務報告を行なうためのシステムの信頼性に係るサービスレベルを定義し、管理する。	委託外注管理規程に基づいて、事前に契約内容を社内で協議しており、サービスレベルについても確認が行われております。又、契約後の品質も定期的に評価しております。	・委託外注管理規程 ・SLA ・契約書 ・委託先の組織図 ・委託内容のフローチャート ・品質評価シート	内部監査人	20xx年 ○月○日	・委託外注管理規程を入手し、サービスレベルの定義、また監視方法等が整備されていることを確認する。	○	・委託外注管理規程に基づいて、システム障害が業務に支障をきたす可能性を考慮し、委託契約でサービスレベルが記述され、このサービスレベルを維持していることを表す文書を確認する。財務報告そのものを委託しているときには、結果としての財務報告の提供がタイムリーか、記載されている情報に誤りがないか検証する部署とプロセスを確認する。	内部監査人	20xx年 ○月○日	・委託外注管理規程に基づいて、システム障害が業務に支障をきたす可能性を考慮し、委託契約でサービスレベルが記述され、このサービスレベルを維持していることを表す文書を確認した。財務報告そのものを委託しているときには、結果としての財務報告の提供がタイムリーか、記載されている情報に誤りがないか検証する部署とプロセスを確認した。	○
	サービスレベルが維持されていることを管理しないと、サービスレベルが低下しても気づかない。	2	委託先のサービスに関する品質の保証内容を管理するための指標を確立する。	委託内容は委託外注管理規程及び事前の会議にて品質の評価基準も決定しております。	・委託外注管理規程 ・SLA ・契約書 ・評価シート ・契約書サンプル	内部監査人	20xx年 ○月○日	・サービスレベルを実際に評価したときの報告書を入手し、主要な性能指標が含まれていて、実際に測定されていることを確認する。	○	整備状況評価と同様の手続となる。	内部監査人	20xx年 ○月○日	整備状況評価と同様の手続となる。	○
	サービスレベルをモニタリングしないと、処理される財務情報の完全性、正確性、正当性が保たれない。	3	委託先業者によって、セキュリティや完全性に対して適切なレビューが行われている。	委託外注管理規程に基づき、外部委託業者と締結したSLAは、都度達成度を測定し評価して記録をとり、責任者に報告しております(モニタリング報告書)。	・SLA ・モニタリング報告書 ・委託外注管理規程 ・契約書 ・評価シート ・モニタリング報告書	内部監査人	20xx年 ○月○日	・委託外注管理規程を入手し、提供されているサービスレベルや成果の評価方法が整備されていることを確認する。	○	・委託外注管理規程に基づいて、提供されているサービスレベルや成果の評価を実施していることを確認する。	内部監査人	20xx年 ○月○日	・委託外注管理規程に基づいて、提供されているサービスレベルや成果の評価を実施していることを確認した。	○
⑤EUC()エントユーザコンピュータティング	EUC開発の際に意図的に不正なプログラムが組み込まれたり、処理の誤りが顕在化する。	1	EUC開発におけるセキュリティ及び処理の完全性について、方針・手続が定まっており、適切に運用されている。	EUC作成の手引きがあり、また作成後に第三者による正確性の検証を行っております。	・システム運用手引書 ・EUC一覧表 ・検証結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、EUC管理手順・体制が整備されていることを確認する。	○	・システム運用手引書に基づいて、EUCが管理され、第三者による正確性の検証を行っていることを確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、EUCが管理され、第三者による正確性の検証を行っていることを確認した。	○
	正確性、完全性等が検証・承認されていないEUCが把握されずに私用されることにより、財務方向の信頼性を阻害する。	2	企業内で使用されているEUCは網羅的に文書化され、然るべく責任者により把握されている。	各部門ごとに使用しているEUCは一覧表が作成され、適時更新されております。	・システム運用手引書 ・EUC一覧表	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、EUC管理手順・体制が整備されていることを確認する。	○	・システム運用手引書に基づいて、一覧表が作成されていることを確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、一覧表が作成されていることを確認した。	○
	バックアップされていないと、データを消失した場合に、復元ができない。	3	ユーザーにより開発されたシステムやデータは、定期的にバックアップを取り、適切に保管されている。	EUCの開発・更改の毎に、データのバックアップをとっており、外部倉庫にバックアップデータを保管しております。	・システム運用手引書 ・対象システム一覧 ・ログ	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、EUCのバックアップの手順・体制・保管方法等が整備されていることを確認する。	○	・システム運用手引書に基づいて、バックアップが行われていることを確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、バックアップが行われていることを確認した。	○
	各EUCの使用・アクセスが自由であると、改ざんなどにより完全性が保たれず、財務報告の信頼性を阻害する。	4	EUCに関して、不正や誤りによる改ざん等を防止するための保護が適切になされている。	情報セキュリティ規程でアクセス権について明記されており、それに基づき利用者の権限を設定しております。利用に関してはログインパスワードの制御を行っております。	・システム運用手引書 ・アクセス権一覧表	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、EUCのアクセス権について手順・体制が整備されていることを確認する。	○	・システム運用手引書に基づいて、EUCのアクセス権について適切な権限が付与されており、第三者がアクセス出来ない対策を行っていることを確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、EUCのアクセス権について適切な権限が付与されており、第三者がアクセス出来ない対策を行っていることを確認した。	○
	EUCの検証なしでは、財務報告への信頼性を担保する完全性・正確性が証明できない。	5	開発されたEUCに関して、入力から出力までの完全性、正確性について開発者以外の独立した者によって検証が行われている。	作成したEUCは、作成者以外の第三者により、その処理の正確性・完全性の検証が行われております。	・システム運用手引書 ・EUC一覧表 ・検証結果報告書	内部監査人	20xx年 ○月○日	・システム運用手引書を入手し、EUC管理手順・体制が整備されていることを確認する。	○	・システム運用手引書に基づいて、EUCが管理され、第三者による正確性の検証を行っていることを確認する。	内部監査人	20xx年 ○月○日	・システム運用手引書に基づいて、EUCが管理され、第三者による正確性の検証を行っていることを確認した。	○