日本内部監査協会

第41期「情報システム監査専門内部監査士」認定講習会

IT統制評価手法のご紹介

2026年6月

GMOフィナンシャルホールディングス株式会社
GMO少額短期保険株式会社出向　内部監査室長
長島　基

目　次

時間の許す範囲でお話します。

時間の許す範囲でお話します。

■お断り

私のコマでは、演習問題を実施する関係で、事前に配布した資料と投影しているスライドが異なります。

事前に答えが分かっちゃうと面白くないから！

そこで、事前配布資料に存在しないスライドの説明の際は、画面に注目してください。

なお、画面に投影したスライド（演習問題の回答を載せた資料を講習終了後に配布しますので、ご安心ください。
事前配布資料に存在しないスライドの内容をメモする必要はありません。

0. はじめに

0-1.講師の略歴

0-2.GMOフィナンシャルホールディングスグループの概要

0-3. GMOフィナンシャルホールディングスの内部監査部門の組織構成

0-4.GMO少額短期保険株式会社の組織構成

0-5.IT統制評価スケジュール

0-1. 講師の略歴

（1）略歴

- 1984年　　：富国生命保険相互会社入社
- 1984年～1997年：システム開発部門に所属し、システム開発等を担当
- 1997年～1999年：経営企画部門に所属
- 1999年～2006年：システム企画部門に所属し、システムリスク管理態勢の構築・運用に従事
- 2006年～2008年：システム子会社に出向し、システム開発部門の課長を務める一方、IT統制整備のフレームワークを策定
- 2008年～2012年：内部監査部門にて本社・関連会社監査および監査企画を担当
- 2012年～2014年：フコクしんらい生命へ出向し、システムリスク管理等を担当
- 2014年～2020年：フコクしんらい生命内部監査部門長
- 2020年～2021年：フコクしんらい生命監査部
- 2021年～2022年：CAICA DIGITAL内部監査室
- 2022年～2025年9月　：フコクしんらい生命監査部
- 2025年10月～　：GMOフィナンシャルホールディングス株式会社　GMO少額短期保険株式会社出向　内部監査室長

0-1. 講師の略歴

(1)略歴

内部監査に係る活動

- 2010年、2017年 : 日本内部監査協会「情報システム監査実践講座」講師
- 2011年 : CIA取得
- 2012年～ : 日本内部監査協会「情報システム監査専門内部監査士認定講習会」講師
- 2014年、2018年 : 情報システムユーザ会連盟主催「システム監査講演会」でパネラーを務める
- 2015年 : 日本内部監査協会　内部監査推進全国大会で「経営に貢献する情報セキュリティ監査」の講師を務める
- 2018年～2020年 : 日本内部監査協会 「内部監査士認定講習会」講師
- 2019年 : 日本内部監査協会 「スキルアップ研修会
  - 失敗する内部監査人10の特性」講師
- 2021年、2023年 : 情報システムユーザ会連盟主催「システム監査講演会」講師
- 2025年 : 日本内部監査協会　情報産業部会、SAM研修会、関西地区監査研究会議「クラウドサービスを対象とした監査手法のご紹介」講師

0-2. GMOフィナンシャルホールディングスの概要

①GMOフィナンシャルホールディングスの概要
https://www.gmofh.com/

②GMO少額短期保険株式会社の概要
https://gmo-minihoken.com/

③親会社であるGMOインターネットグループの概要
https://group.gmo/

https://athletes.gmo.jp/

https://developers.gmo.jp/technology/78173/

0-3. GMOフィナンシャルホールディングスの内部監査部門の組織構成（2026年4月1日現在）

（1）要員構成

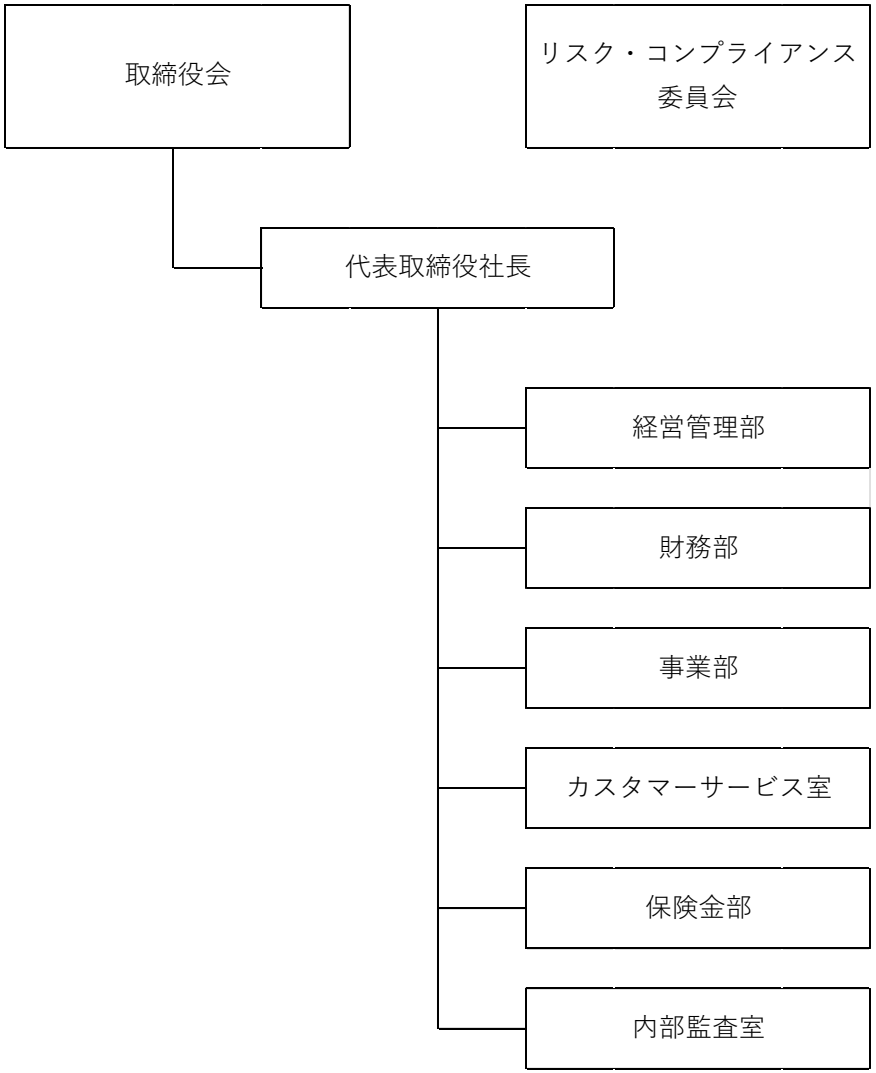
10名

（2）担当業務

・フィナンシャルホールディングス監査
・ホールディングス傘下の複数の事業会社の監査
・財務報告に係る内部統制の評価など

0-4. GMO少額短期保険株式会社の組織構成

（2026年4月1日現在）



（1）要員構成

- 取締役3名
- 監査役
- 従業員8名（内部監査室1名）

（2）内部監査室の業務

- 部門監査
- テーマ監査
- 代理店監査など

0-5. IT統制評価スケジュール

(1)11月:財務報告に係る内部統制有効性評価の通達発信
（自己評価およびサンプル提出期限:3月中旬）
(2)～3月中旬まで:システム所管部門による自己評価
(3)3月中旬～4月末:内部監査部門による評価、評価結果の伝達
(4)4月:システム部門による内部監査部門評価への対応
(5)4月:内部監査部門による追加評価

本日ご説明する内容は、前職で実施していたIT統制の評価を踏まえた同手法のご紹介となりますのでお断りします。

1. 演習問題

システム監査とIT統制評価の類似点と相違点は？

「監査（評価）工程ごとに何が同じで何が違うのか考えてみよう!
同じやり方でよいことと、違ったやり方をしなければならないことを理解すれば、今後の仕事の進め方に役立つはず!?」

1-1.年度計画段階

No.	評価項目	類似点	相違点
1	①監査対象または評価対象	―	システム監査対象は、内部監査部門で任意で設定できるが、IT統制評価では、評価が必要なシステムを対象として網羅的に評価を行う必要がある。
	②監査実施時期または評価実施時期	―	システム監査実施時期は任意で設定できるが、IT統制評価については、評価該当年度を通した評価を実施する必要があるため、サンプル収集時期を考慮すると年度後半に設定する必要がある。
	③要員計画	要員計画に変わりはない。強いていえば、監査は複数要員で比較的短期間で実施し、IT統制評価は少人数で（1人でも可）システムごとに評価していくなど比較的長期間でも問題ないことか。	―

1-2.予備調査またはIT統制評価準備段階

No.	項目評価	類似点	相違点
2	①対象システムのリスク	ー	システム監査では、監査対象システムごとにリスクが異なる。(C:confidentiality(機密性)、I:integrity(完全性)、A:availability(可用性)) IT統制評価では、財務報告が正しく作成されないというリスクを評価する。
	②予備調査必要性の有無	ー	システム監査では、基本的に個別監査の都度、監査対象システムのリスクやコントロールの状況に応じて予備調査を実施する。 IT統制評価では、財務報告が正しく作成されないというリスクに対して、適切なコントロールが行われているかを評価する。したがって、基本的にすべての評価対象システムに対する評価項目は同一であり、事前に評価プログラム(評価手続き)が作成されていて予備調査が不要なことが多い。

1-2.予備調査またはIT統制評価準備段階（続き）

No.	項目評価	類似点	相違点
2	③監査（評価）手続き	システム監査およびIT統制評価において、監査（評価）手続きに変わりはない。監査（評価）にあたり、FISCの『システム監査基準』や経済産業省の『システム管理基準』、『システム監査基準』等のガイドラインを参考にして、監査（評価）手続きを作成して何等問題ない。	ー

1-3.サンプル抽出段階

No.	項目評価	類似点	相違点
3	①必要サンプル数や許容できるエラーに対する考え方	ー	システム監査では、重要なリスクに対しては、サンプル数を多くしたり、様々な切り口でサンプルを用意する。 リスクの大きさによっては、ある程度のエラーを許容できる場合もあるが、1件たりともエラーを許容できないケースもある。 IT統制評価では、コントロールが有効であることが確率的に確認されればOKという考え方でサンプル数を決める。したがって、抽出したサンプルでエラーが発見された場合、さらにサンプル数を増やして評価を行い、エラーが一定の確率の範囲内に納まればOKとし、そうでなければNGとする。

1-3.サンプル抽出段階（続き）

No.	項目評価	類似点	相違点
3	②サンプル抽出時の留意点	ー	システム監査では、リスクが高いであろうと想定されるサンプルを抽出する。例えば、金額が大きいもの、人事異動で担当者が代わったタイミング、イレギュラー取引などのサンプルを抽出する。 IT統制評価では、評価対象期間を通して問題ないかといった観点でサンプルを抽出する。

1-4.実地監査またはIT統制評価段階

No.	項目評価	類似点	相違点
4	①インタビュー、資料の閲覧など	システム監査およびIT統制評価で特に違いはない。敢えていえば、IT統制評価ではインタビューは必須ではないが、システム監査では、通常インタビューなしで指摘はしない。	ー

1-5.監査結果報告書またはIT統制評価記述段階

No.	項目評価	類似点	相違点
5	①指摘の有無（IT統制評価の場合、統制上の不備を指摘してよいか）	システム監査およびIT統制評価で特に違いはない。もちろん、IT統制評価において統制上の不備が発見された場合は、指摘する。	―

1-6.フォローアップ段階

No.	項目評価	類似点	相違点
6	①フォローアップの有無（IT統制評価の場合、フォローアップを行うか）	システム監査およびIT統制評価で特に違いはない。もちろん、IT統制評価において統制上の不備が発見された場合、フォローアップを実施する。	―

1-7.最終的なIT統制評価記述段階

No.	項目評価	類似点	相違点
7	①指摘事項の不備が解消されなかった場合	―	IT統制評価において不備が発見され、最終的な評価段階までその不備が解消されなかった場合、その不備が直接財務報告の正確性に影響を及ぼすと考えるとき、最終的な評価としてその旨を記載する。 一方、最終的な評価段階において、不備が解消されなくとも、当該コントロールを補完するコントロールが存在し、そのコントロールが行われることによって、財務報告の正確性にまで影響を及ぼすとは考えられないとき、最終的な評価としてその旨を記載する。 【記載例】 「20〇〇年〇月〇日付『IT統制評価記述書』にて指摘した項番〇〇については、最終的な評価段階において、改善に向けた取り組みは行われているものの、（改善予定期日：20××年×月×日）20△△年△月△日現在、指摘事項は改善されなかった。しかしながら、本指摘事項については、改善に向けた取り組みが行われていること、ならびに本統制以外に□□□といったコントロールが継続的に実施され本統制を補完していることから、財務報告の正確性に影響を与えるとはいえない状況であると評価する。」

2. ご紹介するIT統制評価の特徴

2-1.評価対象システムおよび評価単位

2-2.自己評価と内部監査部門による評価

2-3.ガイドラインを使用した評価

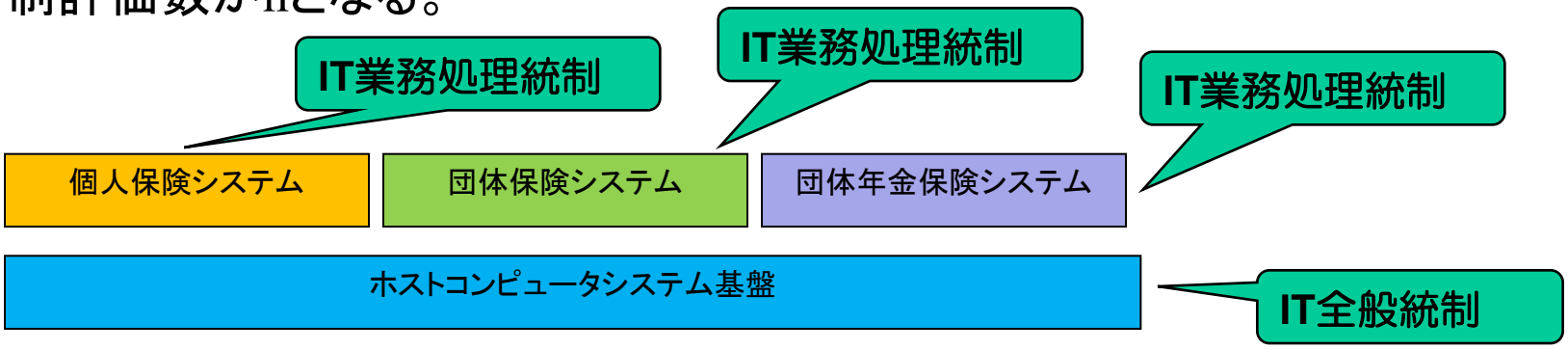
2-1.評価対象システムおよび評価単位

(1) 評価対象システム

・ホストコンピュータおよびクライアント・サーバ上で稼動している個人保険、団体保険、団体年金保険、資産運用システムを対象に評価。

(2)評価単位

・IT全般統制は、システム基盤ごとに評価を実施し、IT業務処理統制は、システム単位に評価している。したがって、複数システムが同一システム基盤上で稼動している場合、IT全般統制の評価数1に対し、IT業務処理統制評価数がnとなる。



2-2.自己評価と内部監査部門による評価

（1） 自己評価

・システム所管部署による自己評価を行い、IT統制評価記述書（RCM)に記載したうえで、必要なサンプルとともに提出してもらう。

（※）IT統制評価記述書（RCM)の記載方法については、後述。

（2） 内部監査部門による評価

・内部監査部門では、必要に応じて任意のサンプルを抽出し、評価を実施する。

2-3.ガイドラインを使用した評価

（1） ガイドラインの使用

・評価に当たり、金融情報システムセンター（FISC）発行の『金融機関等のシステム監査基準』（以下『システム監査基準』）をガイドラインとして使用し、本書を参考にしてIT統制評価記述書（RCM）を作成し使用している。

（2） 評価項目ごとの評価方法

・評価項目ごとの評価方法は、以下の3つの観点で評価している。

①整備（必要なルールが定められているか）

②運用【設計評価】（現在整備されている内容は、留意事項に照らして十分か）

③運用【運用評価】（ルールどおりに運用されているか）

3. IT統制評価にガイドラインを活用することのメリットは？

3-1. IT統制評価にガイドラインを活用することのメリットは？

3-2.活用するガイドラインとして『システム監査基準』を選んだ理由は？

3-1. IT統制評価にガイドラインを活用することのメリットは？

→評価の妥当性を担保できる。

- 評価項目の正当性
- 評価手続きの正当性

（Q）評価項目や評価手続きはどのようにして設定したんですか？（あなたが勝手に決めたんじゃないの？）

（A）（いいえ、私が勝手に決めたのではなく）システム監査やIT統制評価を専門に研究している組織が発行したガイドラインを活用して設定しました。

→評価手続きの設定の容易性

- 監査指針なので、監査人がどのように監査すればよいかチェックポイントに書かれているので、コピーして貼りつければ、そのまま監査手続きとして活用できる。（楽チンだよな！）

3-2. 活用するガイドラインとして『システム監査基準』を選んだ理由は？

◇ガイドラインとしては、ほかに経済産業省『システム監査基準』・『システム管理基準』 などが存在する。

→FISCは常設の組織であり、コンピュータの安全対策やシステム監査等の分野について、必要に応じて継続的でタイムリーに改訂版を発行している。

→入手の容易性。

・PDF版：1,000円。
FISCのHPより購入可能。

※参考として『システム監査基準』システム監査チェックポイント一覧表を添付しますので、ご参照ください。 別紙1

3-2. 活用するガイドラインとして『システム監査基準』を選んだ理由は？

（Q）『システム監査基準』は、金融情報システムセンター（FISC）が発行した書籍であるため、金融機関向けであり事業会社に適用するのは難しいのでは？

（A）『システム監査基準』には、CD/ATM等の管理など一部には金融機関特有の事項が書かれているが、それらを除くとどの業種でも問題なく活用可能な内容である。

※参考として『システム監査基準』と経済産業省『システム管理基準』 の一部（外部委託に係る契約）を添付しますので、ご参照ください。

●『システム監査基準』 別紙2

●経済産業省『システム管理基準』 別紙3

4.ガイドラインを使用したIT統制評価方法

4-1.ガイドラインの位置づけ

4-2.ガイドラインと整備と運用

4-3.ガイドラインを使用した評価方法

4-1. ガイドラインの位置づけ

(1)ガイドラインの位置づけ

・監査を行うにあたって、ガイドラインは仮の評価基準と位置づける。

・システム部門と調整し、ガイドラインを会社として遵守すべき評価基準として設定するか、ガイドラインより下のレベルを評価基準とするか決定する。

※「本章に記載しているチェックポイントは、あくまでも例示に過ぎないため、本チェックポイントを活用する際は、機械的に監査項目として使用するのではなく、リスク特性等を踏まえて取捨選択したうえで、監査項目を作成する必要があることに留意いただきたい。」

(『システム監査基準』P128)

4-2. ガイドラインと整備と運用

(1)社内ルールの整備状況の評価

・現在整備している社内ルール(レベル)で十分かという観点で評価する。その際に、仮の評価基準としたガイドラインとの対比(ギャップ)で評価する。

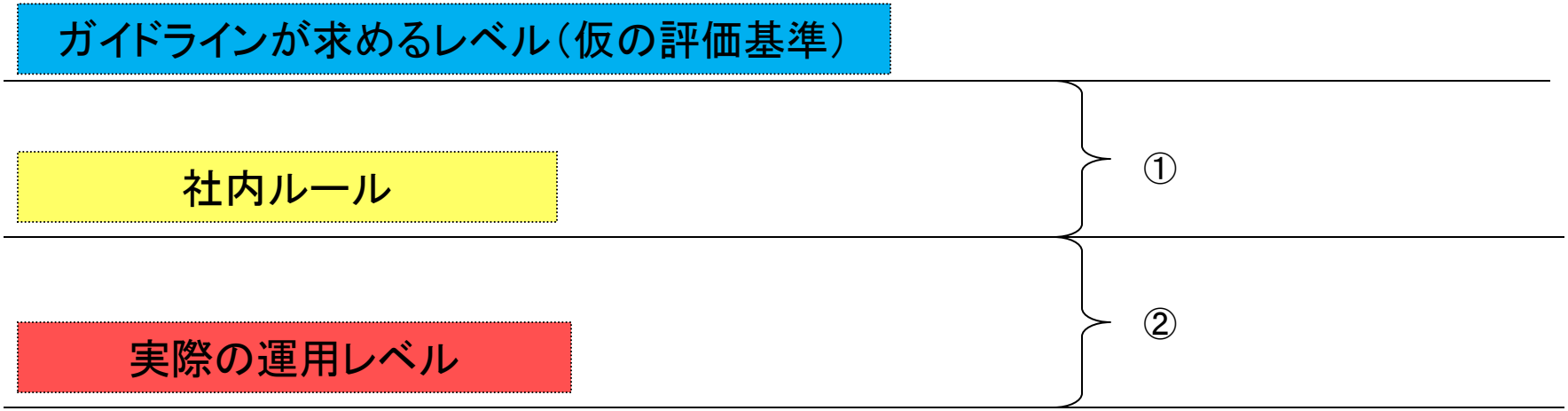
(2)運用状況の評価

・定められた社内ルールを遵守して運用されているかという観点で評価する。

・運用状況には、社内ルールを遵守しているケースのほかに、社内ルール以下のレベルで運用されているケースと、社内ルールに定めはないがそれ以上のレベルで運用されているケースの2通りが存在する。

4-3. ガイドラインを使用した評価方法

(1)実際の運用レベルが、ガイドライン・社内ルール以下のケース



① 社内のリスク管理レベルを上げる必要がないか、ガイドラインの該当ページを提示して(根拠)、システム部門とよく協議して、結論を導く。

ガイドラインの仮の評価基準を評価基準とする？　それとも社内ルールを評価基準とする？

リスク管理レベルの向上について合意が得られれば、IT統制評価記述書の内部監査人の見解欄に推奨事項として、監査結果報告書に記述する。(～することが望ましい。)

② ルール違反であり、指摘事項として指摘する。(～されたい。)

4-3. ガイドラインを使用した評価方法（続き）

(2) 実際の運用レベルが、社内ルール以上のケース

実際の運用レベル

社内ルール

①

① 実際の運用レベルが、社内ルールより上のレベルにあるが、そのような運用を行っている根拠が存在しない。

現行レベルの運用が必要だと判断される場合は、社内ルールの改訂を指摘・推奨する。

現在の状態を放置した場合、異動等で運用担当者が交代したときに、確実に現在のレベルを維持できると考えますか？　規程を整備しておいた方がよくありませんか？

5．IT統制評価記述書（RCM）の構成

5-1.評価項目の選定方法

5-2.自己評価前に記載されている項目

5-3.自己評価時に記載する項目

5-4.内部監査部門による評価時に記載する項目

5-5.フォローアップ時に記載する項目

5-1.評価項目の選定方法

(1)システム子会社の検討チームと富国生命システム企画部門にてどのようにIT統制評価を行うか、ガイドラインとして何を使うかを協議して、『システム監査指針』を活用することに決定。

↓

(2)上記検討チームにて『システム監査指針』のチェックポイント集から評価対象項目をピックアップ。

↓

(3)FISCが策定したRCMのひな型を参考として、RCMの項目案を提示。

↓

(4)上記検討チーム、富国生命システム企画部門、同内部監査部門の協議を経て、評価項目およびRCMの項目を決定

5-2.自己評価前に記載されている項目

(1)『システム監査指針』から記載した項目

- リスク
- 統制目標(留意事項)

(2)FISCのRCMのひな型よりセットした項目

- 整備:運用
- 予防:発見
- 要件(網羅性、実在性…):業務処理統制

(※)IT全般統制評価記述書 → 別紙4

IT業務処理統制評価記述書 → 別紙5

5-3.自己評価時に記載する項目

黄色で塗りつぶした項目です

- 統制の状況
- 回答部署
- 手作業：自動化
- 整備状況（文書、プロセス、システム実装）：全般統制
- 頻度
- 統制評価手続
- 自己評価
- 評価並びに検出事項
- 過年度評価の利用
- 必要サンプル数
- 使用サンプル数
- 調書番号
- 評価日

何年も自己評価を繰り返すと使用したサンプルは異なるものの、記載内容は前年とあまり変わらなくなってきます。
もちろん内部監査人の指摘・推奨事項を受けて、コントロールレベルが向上したものについては、統制の状況をはじめとして記載内容が変わりますが。

5-4.内部監査部門による評価時に記載する項目

ピンク色で塗りつぶした項目です

- 統制評価手続（上書き）
- 評価並びに検出事項（上書き）
- 使用サンプル数（サンプルを追加したとき上書き）
- 調書番号（調書を追加したとき上書き）
- 評価日（上書き）
- 監査部評価結果
- 内部監査人の見解

内部監査部門では、必要に応じて任意のサンプルを抽出して評価し、その結果を監査部評価結果、内部監査人の見解欄に追記する。（4段階評価）

RCMの記載項目が多いこともあり、上書き方式を採ることにより項目数が増えないようにしています。
また、最終的な評価がどうだったのかが重要であり、対象システム所管部門が自己評価をどのように行い、その結果がどうだったのかについては、最終成果物には不要と判断しました。

5-5.フォローアップ時に記載する項目

(1)内部監査人の見解に指摘・推奨項目があったとき

・内部監査人の見解への対応(対応内容(回答)、対応期限)

オレンジ色で塗りつぶした項目ですね

→評価対象システム所管部門が評価後1ヶ月以内に回答

(2)指摘・推奨事項に対する追加評価をしたとき

・内部監査人の見解(追加評価)

紫色で塗りつぶした項目ですね

→内部監査人の見解への対応(対応期限)を考慮し、対応が完了した頃を見計らって評価する。

規程の整備やワークシートの改訂等は比較的早期に対応可能ですが、システム対応が必要となるものは対応に時間がかかることから、対応が完了したものを数回に分けて評価するというかたちになりますね。

5-6.IT統制評価方法の見直し

（1）財務報告に係る内部統制の評価および監査の基準並びに同実施基準の改訂（2023年4月）

①以下の点などを踏まえ、15年ぶりに本基準および同実施基準が改訂された。

- 開示すべき重要な不備が明らかになる事例がみられるなど、内部統制報告制度の実効性に関する懸念が指摘される
- COSO（トレッドウェイ委員会支援組織委員会）の内部統制の基本的枠組みに関する報告書が改訂される（2013年5月）

②IT統制の過年度評価の利用について、以下の留意事項が記載された。

- IT環境の変化を踏まえて慎重に判断し、特定の年数を機械的に適用すべきものではない。

③ IT環境やリスクを考慮し、過年度評価の利用を実施するよう改めた。

5-6.IT統制評価方法の見直し

(2)FISC『システム監査基準』の改訂(2024年9月)

①金融機関等をめぐる環境の変化とシステム監査の重要性の高まりを踏まえて、5年ぶりに本監査基準の改訂が実施された。

②改訂にあたっては、クラウドサービスの利用やサイバーセキュリティ対策に係る個別論点のほか、経済産業省『システム管理基準』等の国内外のガイドラインの最新の内容をもとに見直しが実施された。

③本日みなさんにご紹介している「IT全般統制評価記述書」 別紙4

および「IT業務処理統制評価記述書」 別紙5 については、本監査基準のチェックポイントの改訂内容を反映したものをご紹介しています。

6. ロールフォワードへの対応方法

6. ロールフォワードへの対応方法

(1)ロールフォワードとは？

・評価時点からの変更点を確認し、期中に評価した評価結果を期末日における最終評価結果にするための手続きのこと。

・期中で評価した後に統制環境や統制方法に変更があったか確認し、変更があれば再評価を行う必要がある。

(2)変更の有無の確認方法

・システム管理者に対し、統制環境（財務報告に係るシステムの変更など）や統制方法（IT統制評価記述書の統制の状況欄に記載した内容）に変更があったか質問書を送付し、回答を得る。

・変更がない旨の回答を受領したら、期中で評価した評価結果を最終評価結果とし、本質問書および回答書を証拠として会計士へ提出する。

「証拠として提出できるように、文書でやり取りをするところがポイントですね!?」

7. 効率的で高品質な評価を行うための工夫

7-1.統制の状況

7-2.統制評価手続

7-3.評価並びに検出事項

7-4.内部監査人の見解

7-5.効率的な評価

7-1.統制の状況

（1）自己評価者によって記載レベルに差があるんだよな

（2）必要なことを書いてきてくれない人もいるよね

→それじゃあ、事前に書くべき項目を決めちゃえばいいよね！

→5W1Hで書いてもらったらどう？

→When：ホストコンピュータへアクセスする際には

→Who：システム運用部門では

→Why：不正アクセスを防止するために

→How：「〇〇〇規程」に基づき

→What：△△△を行っている！！

7-2.統制評価手続

（1）これも評価者によって記載レベルに差があるよね

（2）はっきりいって、そのような手続きでは、適切な統制が行われていることを証明できないようなのもあるから困るんだよな

→それじゃあ、内部監査部門でこうやって評価するんだよという内容に上書きしてしまって、次回から同様の手続きで自己評価してもらおう！

→「◎◎◎」を閲覧し、（監査手法：閲覧、突合、比較、質問など）

→「◎◎◎」第×条に定められた〇〇〇どおりに（根拠）

→△△△が行われていることを確認する！（語尾は～する）

7-3.評価並びに検出事項

（1）統制評価手続きに記載された手続きを実施すると、どうしてこういった評価結果になるのか理解に苦しむような記載になってるのがあるんだよな

→でも、前回内部監査部門が上書きした統制評価手続をそのまま実施して、自己評価の際に統制評価手続欄に記載された内容を単純にコピーして、オウム返しのように書けばいいんじゃない？

→「◎◎◎」を閲覧し、

→「◎◎◎」第×条に定められた〇〇〇どおりに

→△△△が行われていることを確認した！（語尾は～した）

7-4.内部監査人の見解

(1)人によってレベルに差があるよな

(2)どこまでが事実(評価時判明事項)で、どこからが監査意見なのかごちゃまぜでよく分からないのがあるよな

(3)不適切な事実をあげて指摘するだけで、どうすればいいか分からないのもあるよね

(4)だから改善が進まないんだよ！

(5)じゃあ、どう書けばいいんだろう？

→まず第一に、リスクに対する統制目標に対して、どのような統制状況だったのか確認した事実を書き、

→それに対する監査意見を表明し、

→どう改善すればよいか具体的に提案するのがいいよね！

7-4.内部監査人の見解(続き)

(1)リスク:関係する役職員がセキュリティ対策を実行できない

(2)統制目標:セキュリティスタンダードを関係する全役職員に周知徹底すること

→今年度の階層別研修実績は2回であり(事実)、

→セキュリティスタンダードの周知徹底は不十分である。(意見)

→関係する役職員が理解しておくべき情報セキュリティに関する具体的な教育実施計画を策定し、(改善提言)実施されたい。

→(監査人:情報セキュリティ教育に関する年度ごとの(十分な内容の)教育実施計画を策定し、実施すれば指摘事項は改善されたと評価します。被評価者:分かりました。計画を立てて実施します。)

7-5.効率的な評価

串刺し評価がオススメ！！

（1）IT統制の評価については、評価対象のシステムも多いし、結構負担だよな

（2）内部統制評価制度開始当初は、きっちりやってくれという感じだったけど、最近はもっと短時間で効率的にできないかという要請も強くなってるよね

→自己評価を活用して効率的にやろう！

→事前に要請しておいて、サンプルの証拠書類を提出してもらおう！（RCMに調書番号を記載してもらい、一覧表添付のうえ各調書にはインデックスをつけて提出してもらうと効果的です）

→システムごとに評価するのではなく、評価項目ごとに各システムを串刺しにするように評価していくと効率的です。

→評価項目の削減に取り組むのも一考かと。

時間の許す範囲でお話します。

8.IT統制評価上のポイント
よくありがちな不備！！
8-1.IT全般統制上の不備
8-2.IT業務処理統制上の不備

8-1.IT全般統制上の不備

(1)当社としてのシステム開発およびシステム運用のルールが定められているか

→システム開発およびシステム運用を外部委託している場合、外部委託先が作成した外部委託先用のルールは存在するが、そのルールは、当社の内部統制上の必要なルールとなっていないことがある。

その場合、必要な社内の承認手続きが定められておらず、結果として内部統制上必要な決裁が行われていることが証明ができないことにつながる。

(2)外部委託先が社外からリモート・アクセスする際のルールが定められているか

→誰がいつ何の目的でどこにリモート・アクセスするかを事前に申請させ、社内での承認を行ったうえで(緊急時の対応は事後でも可)アクセスを許可するというルールを定めて運用する。

また、1ヶ月に1度程度アクセスログと上記申請書を突合し、未承認のアクセスがなかったか確認することが望ましい。

8-1.IT全般統制上の不備（続き）

（3）必要なバックアップが取得され、安全に保管されているか

→必要なバックアップが取得されており、不測の事態が発生した場合、それらを使用して、システムを復旧できるか。バックアップサイクルは適切か。磁気記録媒体が読めない場合を想定して正副の媒体を作成しているか。システム設定情報のバックアップを取得していないと、システムの復旧に時間がかかることが想定される。

→保管場所は安全か。（できれば同一の災害で同時に被災しない場所に保管しておくことが望ましい。）

（4）臨時処理に対するシステム運用ルールが定められ、必要な承認が行われているか。

→システム利用部門またはシステム開発部門からの申請に基づき、システム運用部門の管理職が承認したうえで臨時処理を行うといったルールを定めて運用することが必要。

また、臨時処理実行後は、処理結果に問題はなかったか、臨時処理前後の処理への影響がなかったかの確認を行うことが必要。

8-2.IT業務処理統制上の不備

(1)イレギュラーなデータベースの更新について、ルールが定められ、適切な運用が行われているか

→データベースに格納された項目の値に誤りがあり、通常のオンライン処理などで該当項目を更新できない場合、システム部門等に依頼しイレギュラーな更新を行う場合がある。

その際、データベースの更新に関し、申請、承認、結果の検証、証跡の保管などについて権限者の統制を含めて記載したルールが定められていることが必要であり、IT統制評価の際は、証跡を取得し、適切なコントロールが行われていることを確認する必要がある。

(2)複数のシステム間で受け渡しを行うファイルのインターフェースの不整合により、正しい処理が行われないということはないか

→複数のシステムを接続する場合、接続ファイルのインターフェースに関する検討および調整が不十分なケースや接続ファイルの項目の理解不足により、正しい処理がなされない恐れがある。テスト計画の際に接続テストを計画するようルール化し、ルールどおりテストが実施されているか確認する。

9.おまけ

時間の許す範囲でお話します。

クラウドサービスを対象とした監査手法のご紹介

9-1.クラウドサービスの利用が拡がる背景

9-2.クラウドサービスを対象とした監査のポイント

9-3.具体的な監査計画策定方法

9-1.クラウドサービスの利用が拡がる背景

クラウドサービスか。

ウチの会社でもZoomを使っているけど、これもクラウドサービスの利用だよな。

どのような背景があって、クラウドサービスの利用は拡がってきたんだろう？

9-1.クラウドサービスの利用が拡がる背景

ユーザ部門

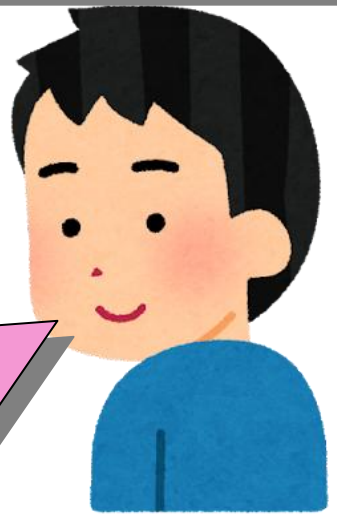
経費精算のクラウドサービスを導入したいんです。よろしくお願いいたします。

情報システム部員

経費精算か。

今使っている会計システムは古いし、使い勝手が悪いもんな。

こんな風にうるうるしながら頼まれたら、断れないよな。



9-1.クラウドサービスの利用が拡がる背景

ユーザ部門

勤怠管理サービスの導入お願します。

よろしくお願いします

福利厚生サービスの導入お願します。

よろしくお願いしま

新入社員の採用管理サービスの導入お願します。

えーっ！

こんなにたくさんの申請が上がってくるの？

セキュリティチェックのフレームワークも整ってないのに、どうしたらいいの？

情報システム部員

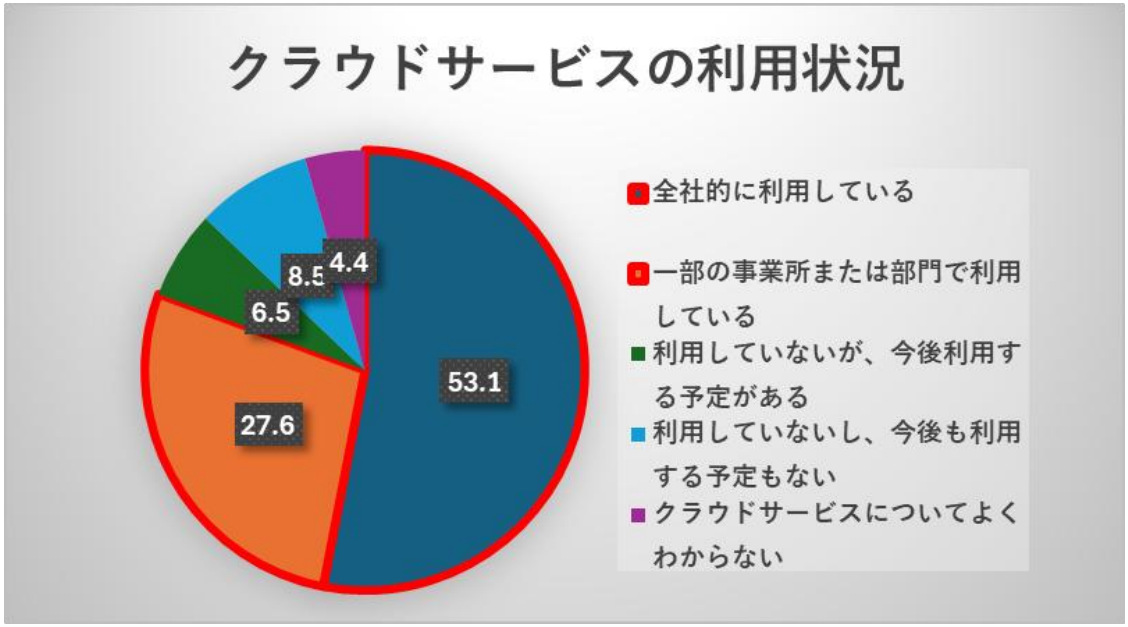
9-1.クラウドサービスの利用が拡がる背景

クラウドサービスの利用申請がたくさん来て、情報システム部は大変そうですが、クラウドサービスの利用が拡がる背景を解説します。

それでは、以下の総務省公表の資料を確認してみましょう。
ウフッ♡

「令和6年通信利用動向調査の結果」総務省　令和7年5月30日公表
https://www.soumu.go.jp/johotsusintokei/statistics/data/250530_1.pdf

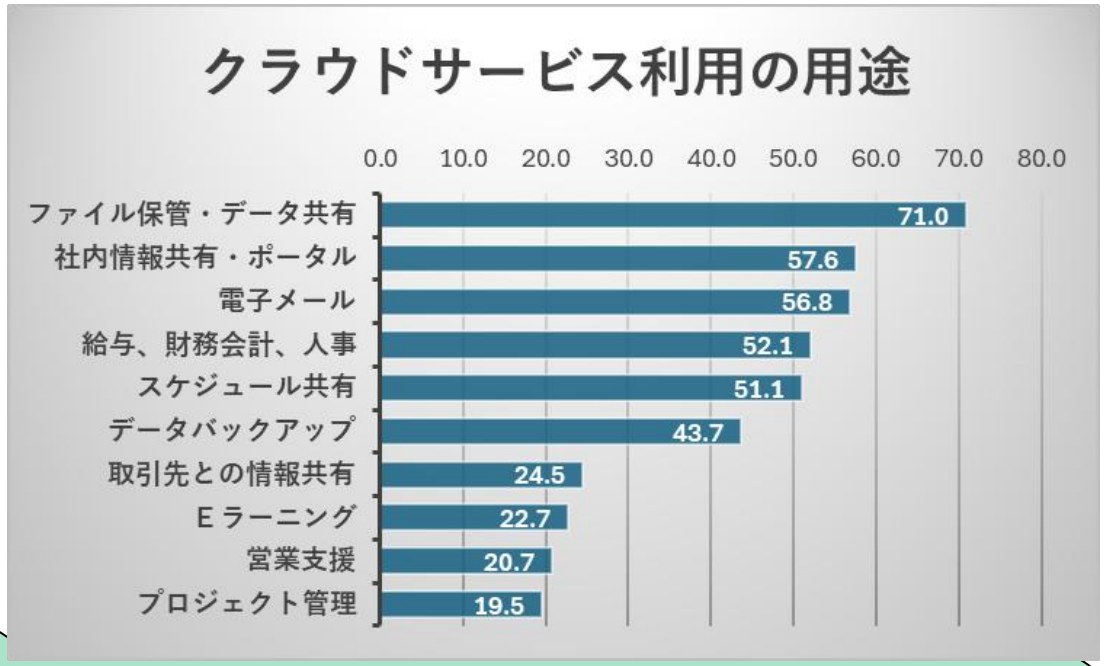
9-1.クラウドサービスの利用が拡がる背景



まずは、クラウドサービスの利用状況です。

「全社的に利用している」と「一部の部門等で利用している」を合わせると80%以上の企業でクラウドサービスを利用しているとの結果です。

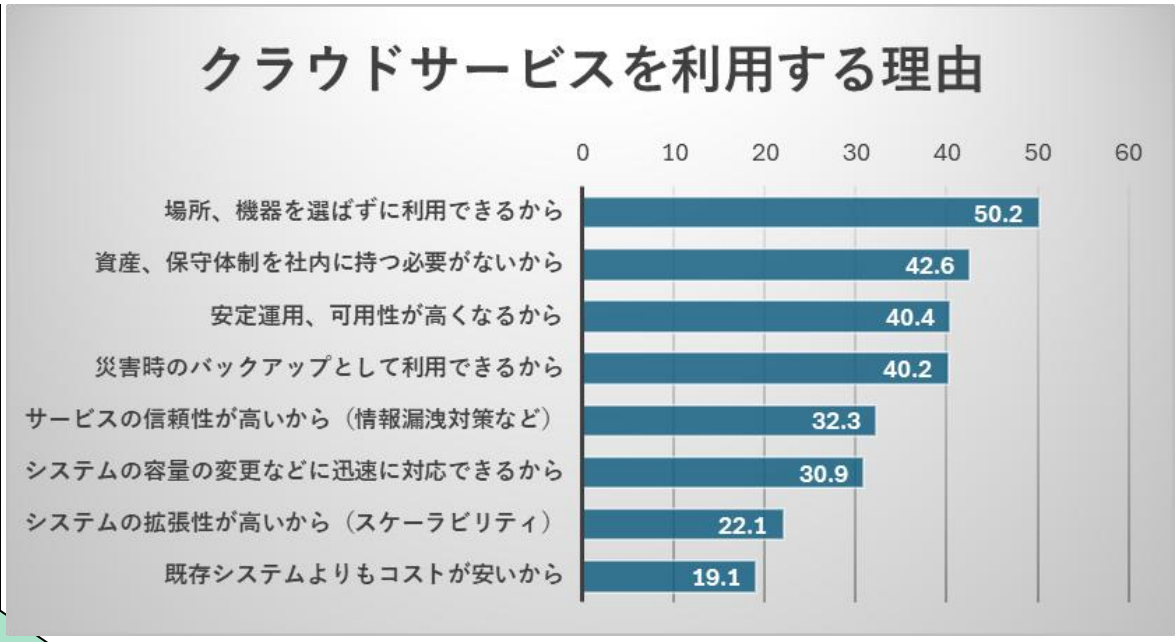
9-1.クラウドサービスの利用が拡がる背景



次に、クラウドサービスの利用用途です。

ファイル保管・データ共有等自社情報の活用で利用されているほか、給与、財務会計、人事、営業支援など業者が提供するアプリケーションの利用にも使われていることが分かります。

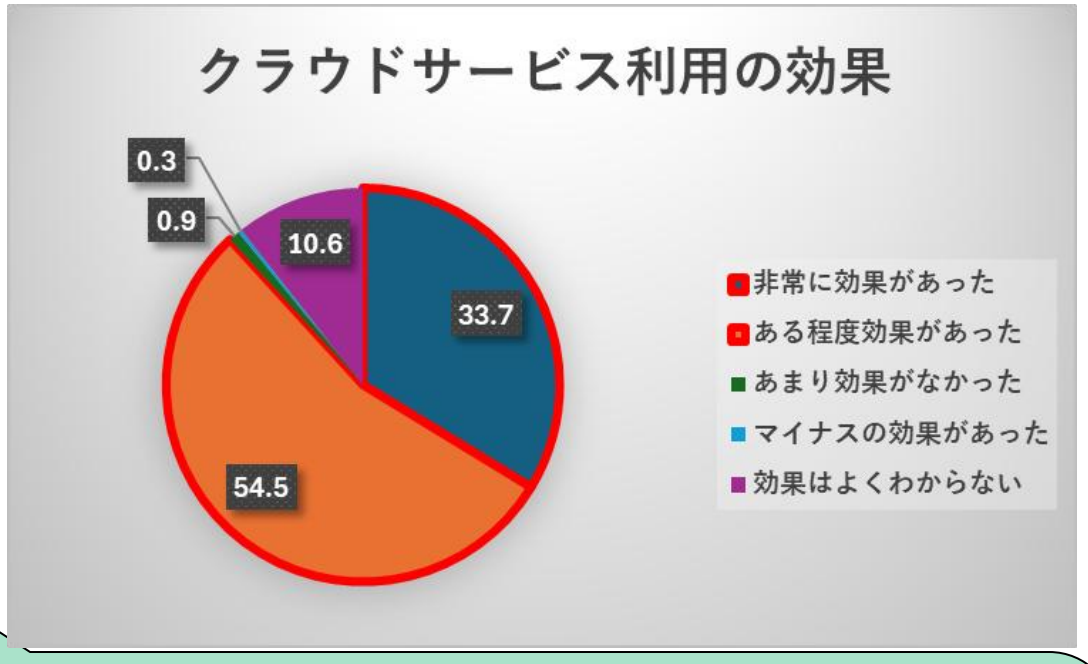
9-1.クラウドサービスの利用が拡がる背景



クラウドサービスを利用する理由を確認してみましょう。

社内にリソースを持つ必要がない、システムの可用性や信頼性が高い、拡張性に優れているなどのほか、コスト面での優位性もサービス利用の理由に挙げられていますね。

9-1.クラウドサービスの利用が拡がる背景



次に、クラウドサービスの効果についてどのように評価しているのでしょうか？

「非常に効果があった」と「ある程度効果があった」を合わせると88%を超えますので、利用企業の満足度が高いことがうかがえます。

9-1.クラウドサービスの利用が拡がる背景

クラウドサービスの利用が拡がる背景について、ご理解いただけたでしょうか？

本サービスの利用企業が80%を超えていることを踏まえるとシステム監査の対象にせざるを得ないといえるかもしれません。

また、そもそも外部委託自体が増えていて、その委託先が利用するシステムがクラウドサービスに置き換わっていることも影響しているのではないかと思われます。

9-2.クラウドサービスを対象とした監査のポイント

なるほど。

ウチの会社でもZoomを使っているけど、監査する際にはどんなところがポイントなんだろう。

しっかり確認しておかなくちゃ！

9-2.クラウドサービスを対象とした監査のポイント

それでは、ここからは、実際にクラウドサービスを対象とした監査を実施した私が説明しましょう。

個々の内部監査の計画では、まずはじめに監査対象（候補）プロセスに内在するリスクの洗い出しと評価を実施しますが、クラウドサービスに係るプロセスには、どのようなプロセスが存在するでしょう。

9-2.クラウドサービスを対象とした監査のポイント

私は、以下の3つのプロセスが存在すると考えました。

1.クラウドサービス導入プロセス

2.サービス契約期間中のプロセス

3.サービス終了プロセス

では次に、それぞれのプロセスに内在する主要なリスクとはどのようなものでしょうか？

9-2.クラウドサービスを対象とした監査のポイント

私は、右のように考えました。

1.クラウドサービス導入プロセス

①有効でないサービスの導入
②必要なサービスレベルを確保できない
③委託先の財務内容などサービスの継続性に疑問がある
④不利益な内容で契約してしまう
⑤サービスの導入が報告されない（可用性などでどのようなリスクをテイクしているのか分からない）

2.サービス契約期間中のプロセス

委託先に対する適切な点検が行われない

3.サービス終了プロセス

①情報報漏洩が発生する
②サービスの終了が報告されない

9-2.クラウドサービスを対象とした監査のポイント

次に、クラウドサービスには、特別な特徴があることを発見しました。

その特徴とは、どのようなものでしょうか？

9-2.クラウドサービスを対象とした監査のポイント

クラウドサービスは2階建て！！

クラウドサービス提供業者

クラウドインフラ提供業者

クラウドインフラ提供業者に内在するリスクとクラウドサービス提供業者に内在するリスクがある。

クラウドインフラ提供業者に係るリスク

①物理的安全管理措置に係るリスク

②データセンター所在地（海外？）に係るリスク

③立入監査可否または第三者評価機関による監査保証書（SOCレポート等）の入手の有無

④可用性リスク（設置されている機器がどの地域（東京と大阪リージョンなど）のどのデータセンター（複数のアベイラビリティゾーンなど）に設置されて冗長化されているか）

9-2.クラウドサービスを対象とした監査のポイント

クラウドサービス提供業者

クラウドインフラ提供業者

クラウドサービス提供業者に係るリスク

①財務の健全性

②各種認証の取得および更新状況

- ISO/IEC27001、同27017、同27018
- プライバシーマーク認証

③脆弱性診断およびペネトレーションテストの実施＆問題点の速やかな解消

③技術的、組織的および人的安全管理措置に係るリスク

④可用性リスク（冗長化対象機器および機器の設置場所）等

⑤契約内容に係るリスク（サービス終了時にデータ消去証明書等の発行が可能か等）

9-2.クラウドサービスを対象とした監査のポイント

クラウドサービスを対象とした監査を実施して右のような感想を持ちました。

① 大手のインフラ提供業者を利用していると安心ですね。

② サービス提供業者については、以下の点がポイントでしょう。

- 情報セキュリティに係る公的な認証を取得し更新しているか
- 個人情報を委託先に格納する場合は、プライバシーマーク認証を取得し更新しているか
- 脆弱性診断やペネトレーションテストを定期的に実施し、必要な対策を速やかに打っているか

9-2.クラウドサービスを対象とした監査のポイント

サービス提供業者についてのポイントは、すべて第三者による認証やテスト等ですね。

第三者による認証や評価を取得している場合、個別のセキュリティレベルの検証の一部をこれらによって、代替できると考えられるかもしれません。

また、これらの認証や評価を取得していないと、サービスの選定の際に選ばれなくなり、淘汰されていくかもしれません。

それからクラウドサービス提供業者の競争が発生し、業者を乗り換える動きが出てきています。そうするとサービスの終了時にデータの消去がなされたことを確実に確認することが重要だと感じました。

9-2.クラウドサービスを対象とした監査のポイント

9-2.クラウドサービスを対象とした監査のポイント

それは大変ですね。

クラウドサービスに預けていたデータが漏洩しちゃったんですって。しかも運転免許証やマイナンバーカードの情報も含まれていたんです。

9-2.クラウドサービスを対象とした監査のポイント

そうなんですね。

それは考えないといけませんね。

担当者に聞いたら、委託先が公的認証を取得していたから安心していたっていうんです。

公的認証を取得しているからって、安心しちゃダメなんじゃないですか？

9-2.クラウドサービスを対象とした監査のポイント

今回の事例を受けて、どういったことが必要なのか考えてみましょう。

まず、一点目は預けるデータの重要度ではないでしょうか？

情報漏洩リスクを考えて、重要度の高いデータを預ける場合は、より慎重にリスク評価を行う必要がありそうです。

二点目は、脆弱性診断とペネトレーションテストに注目したいですね。どのような業者に委託してどのようなテストを実施したのか。その結果、どのような脆弱性が発見され、その問題は解決済みなのかを確認する必要があると思います。

9-2.クラウドサービスを対象とした監査のポイント

三点目は、そのサービスの利用実績でしょうか。日本を代表するような企業が複数利用していれば、利用企業のリスク評価に合格していると考えられますので、この点も確認した方がよさそうです。

四点目は、万が一漏洩した場合に備えて、データを暗号化してクラウドサービスに保管することも有効な対策だと思います。

9-2.クラウドサービスを対象とした監査のポイント

いずれにしても、クラウドサービスを利用するということは、メリットだけでなく、リスクも存在することをよく考えて、慎重に判断する必要がありそうですね。

これは大変失礼しました。

事件の後にもっともらしいことをいうんじゃなくて、事件の起こる前に言ってほしかったわ！

9-2.クラウドサービスを対象とした監査のポイント

みなさん、いかがでしたか？

クラウドサービスを対象とした監査のポイントを理解いただけましたでしょうか？

9-2.クラウドサービスを対象とした監査のポイント

なるほど。

クラウドサービスは2階建てなんだ。

でも、長島さんってすごいよな。誰にも頼らずにこんな監査計画を作れるんだから。

自分みたいに監査経験の乏しい人間には、なかなかマネできないな。

9-2.クラウドサービスを対象とした監査のポイント

それでは次に、長島さんがどのようにして監査計画を策定したのかご紹介しましょう。

あ～ら、そんなに褒めていただいても何にも出ませんことよ。

でも実は長島さん一人で考えたんじゃないんですの。

前述のFISCの『システム監査基準』の要点項目10外部委託に記載されたチェックポイントを参考にしたんですよ。

9-3.具体的な監査計画策定方法

監査計画の策定は、以下のステップで実施しました。

①何をどのように確認すればよいのかの確認

②監査計画書の作成

③監査プログラムの作成

それでは、①の何をどのように確認すればよいのかの確認について、どのように実施したのかご紹介しましょう。

使うのは、これまでにご説明してきたFISCのシステム監査基準のチェックポイント集です。

クラウドサービスについては、要点項目10外部委託にチェックポイントが記載されていますので、そちらを確認します。

9-3.具体的な監査計画策定方法

そして、要点項目10.外部委託は、以下のように区分されています。

それでは、ここからは、実際にどのようなことを実施したのか、当時使用したチェックポイント集（【別紙6】）をご覧いただきながら、ご説明しましょう。

要点項目	大項目	小項目
10.外部委託・外部サービス	1. 外部委託方針・計画	A.外部委託方針・計画
		B.契約締結時
	2. 外部委託業務管理	A. 契約期間中
		B.契約終了時
	3. サービス固有	A.クラウドサービス
		B.共同センター
		C.外部サービスとの連携

9-3.具体的な監査計画策定方法

いかがだったでしょうか。チェックポイント集の使い方をご理解いただけたでしょうか？

それでは、ここからは、今、ご説明しましたことを振り返りましょう。

(1)監査対象プロセスにどのようなサブプロセスが存在するのかの確認

チェックポイント集の大項目や小項目を確認して、監査対象プロセスにどのようなサブプロセスが存在するのかを確認します。

(2)サブプロセスに存在するリスクと必要なコントロールの把握

そして、チェックポイント集のリスク欄とコントロール欄の記載内容を見て、クラウドサービスの利用には、どのようなリスクが存在して、どのようなコントロールが必要なのか確認します。

9-3.具体的な監査計画策定方法

このようにして、(1)～(3)までの作業を実施することによって、監査対象サブプロセス、存在するリスクと必要なコントロール、監査で確認すべきポイントの対象候補が出そろったら、監査リソースと相談して、リスクの大きいサブプロセスおよび監査項目を監査対象として決定します。

(3)監査で確認すべき項目の取捨選択

次に、チェックポイント集のチェック欄の記載内容を見て、クラウドサービスに関係なさそうなことや自社の業種や規模などを考慮すると確認対象外としていいと考える項目などを除外(×)します。

そして、このリスクに対するコントロールは重要だとか、この項目は確認した方がいいなと考える項目を確認対象候補(〇)とします。

9-3.具体的な監査計画策定方法

そうすると、監査対象サブプロセスおよび監査項目が決まりましたので、それをもとに②「監査計画書」を作成します。

監査目標には、この監査で、何を確認したいのかを記載します。

それから、監査範囲には、本監査で確認するスコープを記載しますが、先ほどチェックポイント集をもとに選定したサブプロセスを監査範囲として記載しますが、本サブプロセスのすべてを監査対象とせず、一部のプロセス（監査項目）を対象外とした場合は、「〇〇プロセスを除く」と記載します。

それでは、本監査で実際に作成した「監査計画書」（【別紙7】）をご覧いただきましょう。

このようになっております。

9-3.具体的な監査計画策定方法

次に実施するのが、③の監査プログラムの作成ですが、本チェックポイント集のリスク、コントロールおよびチェックポイントをコピーして、監査予備調書に貼り付けます。

そして、貼りつけたままでは、自社の状況にフィットしないところがありますので、必要に応じて加筆修正します。

また、本チェックポイントには、以下のように記載されています。

10.1. B.契約締結時

1. 次のような手順に従い、外部委託契約が締結されているか。

私が、監査プログラムを作成する際には、監査対象部門に提出してもらう資料やサンプルを加筆します。例えば、こんな風にです。

「クラウドサービスに係る外部委託契約書（直近で契約した10件）および決裁関係書類を閲覧し、以下の手続きが実施されていることを確認する。」

9-3.具体的な監査計画策定方法

なお、私が本監査を実施した際に使用した「システム監査基準」は、2019年3月版ですが、先ほど申し上げたとおり本基準はその後2024年9月に改訂され、第2版が刊行されました。参考までに第2版のチェックポイント集の10.外部委託・外部サービス（【別紙8】）を添付しましたので、ザッと確認してみましょう。

本改定後のチェックポイント集では、【クラウドサービス利用の場合】のチェックポイントが追記されていたり、小項目に10.3. A.クラウドサービスが追記されています。黄色でマーカーを引いた部分ですね。

やはり、クラウドサービスの利用の浸透に応じてリスクが大きくなり、システム監査で取り上げる必要が高まっているといえると思います。

9-3.具体的な監査計画策定方法

ハーイ。クラウドサービスを対象とした監査における監査計画の立案方法を長島さんに説明していただきました。

長島さんの説明を聞くと、かなり「システム監査基準」のチェックポイント集を活用していますね。

したがって、長島さん独自の監査手法ということではなさそうです。

このようなやり方なら、本日講習会にご参加いただいている方々でも真似できそうな気がしますが、いかがですか？

長島さんは、こうもいっていました。「はじめての取組みは誰でも怖いけど、だまされたと思って、まずはやってみることが重要だ！」

10. 最後に

10.最後に

私は、内部監査は面白いと思いますし、会社や社会のために役立つものだと思います。
一方で、内部監査人は、孤独であったり、社内での認知度が低かったり、監査対象部門の人からひどいことをいわれても我慢しなければならなかったりと、つらいこともままあると思います。

しかしながら、内部監査は、組織体の運営に価値を付加するようないわゆる経営監査が求められる時代になってきたのも事実です。

したがって、こういった機会を利用していただき、内部監査人のネットワークを活用して、社外にある知識やノウハウを得てみなさんの内部監査業務に活かしていただけたらと思います。
みなさん、頑張りましょうね！！

おしまい！

ご清聴いただき、
ありがとうございました。
またどこかでお会いしましょう！
再見！！