TOPCERTIFIER
www.topcertifier.com

サービス方法論
SOC 認証用

サービス組織の管理

TOPCERTIFIER
www.topcertifier.com

SOC レポートとは何ですか?

SOCレポート 企業が独立した第三者保証を通じて検証する方法です。サービスプロバイダーは適切な管理を実施しており、事前に業界標準に従っています。ビジネス機能をその組織にアウトソーシングすること。これによりサービスプロバイダーにチャンスが与えられます顧客、投資家、ビジネスパートナー、監査人との信頼を確立し、構築するため 市場での競争上の優位性を獲得しながら。すべてのSOC検査が実施されます に従って

AICPAガイドライン :

その過程で **SOCの実装** 経験豊富なテクノロジーコンサルタントのチーム そして監査人は組織のリーダーと緊密に連携して、次のことを保証します。

- 最終的な SOC レポートは、組織固有のニーズに徹底的かつタイムリーに合わせて作成されます
- 業務運営と内部統制プロセスが合理化されます
- 契約上の義務と市場の懸念が満たされる
- AICPA の報告要件を満たしている

SOC レポートのタイプを決定するにはどうすればよいですか私のビジネスニーズ?

SOC の評価と認定を受ける主な理由は 2 つあります。

- 顧客、見込み顧客、または監査人が SOC レポートを要求する
- あなたの組織は、社会的コンプライアンスを積極的に獲得することを決定しました

最初のシナリオでは、要求者は必要な SOC レポートの種類を指定する可能性があります。どちらでも このシナリオでは、組織はまず目標を考慮する必要があります。通常、どのような場合でも望ましい結果は、組織は、適切な設計と効果的な運営に対する取り組みを実証する必要があります。内部統制環境の改善。

TOPCERTIFIER
www.topcertifier.com

SOC 1、2、3の比較表

SOC レポートには、SOC 1、SOC 2、および SOC 3 の 3 つの異なるタイプがあります。各レポートは異なりますが、関連するリスクと内部統制を評価するために必要な貴重な情報を提供します。アウトソーシングされたサービスプロバイダーを使用して。調査するには独立した第三者監査人が必要です 最終報告書を作成する前に、組織のさまざまな側面を確認します。

SOC 1	SOC 2	SOC 3
社内のレポート 財務関連の管理 情報または声明	内部統制に関するレポート 5つの信託サービスに関すること 原則: セキュリティ、可用性、 誠実さ、機密保持、プライバシー	の結果報告 SOC 2 を適切な方法で 一般の聴衆に向けて
主に監査役と共有	主に顧客に共有され、利害関係者	一般公開
企業にも適用可能 どのプロセスの財務 医療などの情報 請求処理、給与計算 サービス、融資会社 等	あらゆるテクノロジー企業に適用 可能 それは情報処理です。 製品ベースとサービスベースの両方 企業	あらゆる一般人に適用 可能を持っている企業 SOC 2 が検証済みで必要 ですSOC 3 レポートを作 成するには より多くの 一般視聴者に向けて

TOPCERTIFIER
www.topcertifier.com

SOC 1 認証

SOC 2 レポートは、ユーザー企業の財務に関連する組織の管理に焦点を当てています。報告。専門的な理解が必要な非常に詳細な検査です。産業および関連する制御環境。通常、サービス組織は次のように指定します。実行する特定のサービスに基づいた管理目標および関連する管理活動。

SOC 1 レポートには通常、実行に関連するビジネス プロセス制御が含まれます。 SOC1 レポートには通常、以下の完全性と正確性を含むビジネスプロセス管理が含まれます。トランザクションだけでなく、ネットワーク セキュリティや
論理アクセス。

範囲が限られているため、SOC 1 レポートは、
顧客の財務データの管理と保護に自信を持っています。それはよくあることです
ユーザー企業が上場されており、SOX 404 または同様のものに準拠する必要がある場合に必要 規則。以下にいくつかの例を示します


記録管理 サービス


医療請求 処理


給与計算サービス


貸出サービス

TOPCERTIFIER
www.topcertifier.com

SOC 2 認証

SOC 2 レポートは、ユーザー エンティティが必ずしも応答しないサービス組織を対象としています 財務報告の管理を強化し、プロバイダーがより幅広いニーズに対応できるようにします ユーザーエンティティ。

SOC 2 試験は主に、データの保存と保護の方法、具体的にはどのように行われるかに焦点を当てます。AICPA に基づくサービスコミットメントおよびシステム要件に関連する管理トラストサービス基準 (以下に定義)。

- **安全** - 情報とシステムは不正なアクセスや開示から保護されています 情報の

- **可用性** - 情報とシステムは、企業の要求を満たすために運用および使用できるようになります。目標

- **処理の完全性** - システム処理が完了し、有効で、正確で、タイムリーであり、企業の目的を達成する権限を与えられている

- **機密保持** - 機密として指定された情報は、企業の要求を満たすように保護されます。目標

- **プライバシー** - 個人情報は次の目的で収集、使用、保持、開示、廃棄されます。エンティティの目的

SOC 2 レポートは、情報に関心のあるテクノロジー企業であれば誰でも利用できます。処理。 SOC 1 レポートと SOC 2 レポートは両方とも対象読者が制限されていますが、SOC 2 レポートは 見込み顧客、ベンダー管理専門家、規制当局やその他の主要なビジネスパートナー。

SOC 3 認証

SOC 2 と同様に、SOC 3 レポートは、AICPA の 5 つの信頼サービスに関連する管理に焦点を当てています。カテゴリー。ただし、SOC 2 とは異なり、SOC 3 レポートは認定されており、公的に作成できます。利用できるため、管理の有効性をマーケティングするための貴重なツールになります。 環境。

SOC 3 レポートが必要な場合、組織はまず SOC 2、タイプ 2 を完了する必要があります。検査（レポートの種類については以下で詳しく説明します）。 SOC2、SOC3検査が可能 1 つ以上の信頼サービス カテゴリに基づいて。 SOC 3 レポートにはほぼ同じ内容が含まれます SOC 2 レポートに含まれる情報。ただし、詳細な説明が含まれていないものは除きます。コンプライアンスと運用に関連する管理。また、特定の制御も含まれていません。活動、テスト手順、または運用効率に関する詳細な結果。

タイプ 1 とタイプ 2

すべての SOC レポート (SOC 3 を除く) は、タイプ 1 またはタイプ 2 のいずれかになります。違いは次のとおりです。主に対象期間に基づく

- **タイプ 1 レポート：** タイプ 1 レポートは、サービス組織の適合性を説明します。特定の時点でのコントロールの設計と実装。

- **タイプ 2 レポート：** タイプ 2 レポートは、定義された管理活動が一貫して行われていることを保証します。通常 6 か月から 1 年の期間である定義された期間にわたって効果的に運用され、したがって、運用パフォーマンスが向上します

多くの場合、サービス組織はコントロールを定義するためにタイプ 1 レポートから始めます。ある時点でのアクティビティ。コントロールが設計および実装されると、タイプ 2 がレポートが続きます。タイプ 2 レポートは一定の期間 (つまり、6 か月または 12 か月) をカバーするため、このレポートは次のようになります。期間中にコントロールが動作していたことが保証されるため、ユーザーにとってより価値があります。 効果的に。
組織は通常、監査会社に依頼してタイプ 2 レポートを作成します。 毎年。

TOPCERTIFIER
www.topcertifier.com

SOC 評価の準備はどのようにすればよいですか?

最初の SOC 評価を開始するときは、選択したサードパーティと協力することが有益です。私たちのようなコンサルタントが最初のギャップ評価を実行し、ギャップを修正できるようにします。SOC 報告プロセスの開始前。このルートを選択すると、既存のものを埋めるのに役立ちます 現在のシステムのギャップを解消し、より準拠性の高い、非常に近いシステムを実現します。SOC要件を満たすために。各 SOC レポートの範囲は異なりますが、特定の事項があります。すべての SOC 評価に不可欠な重点分野。以下のタスクに焦点を当てることで、組織は従業員をより強力な管理環境に向けて準備し始めることができ、したがって、より効率的な SOC 評価が可能になります。

文書化

監査人の観点からすると、文書化されていないものは存在しないことになります。あるかもしれないが 強力な内部統制が整備されていないと、発生の証拠が記録されない可能性があります。確保するすべての管理をサポートするために文書が維持されます (例: アクセス許可の承認、従業員の謝辞、人口の維持など）。

定義されたポリシーと手順

すべての関係者が組織の使命を果たすための責任を理解するようにするため 目的を達成するために、基本的なプロセスと手順が文書化されていることを確認します。これにより、従業員と監査人の両方が組織内の意図を理解するためのリソース 制御環境。ポリシーの範囲には以下を含める必要があります。

» 契約上の義務を果たすための組織的な手順

» 主要なサービス義務とシステム要件を満たす手段

» リスク管理アプローチ

リスクアセスメント

年次リスク評価の議論によって促進され、承認された正式なプロセス取締役会または経営陣が存在する必要があります。正式な年間リスクの代わりに評価に応じて、組織は四半期ごとに会議を開催して、変更について話し合うことも選択できます。脅威、事業運営など、およびそれらが全体的なリスク評価に及ぼす影響。リスク評価には、定義されたリスク レベル (つまり、低、中、高の脅威) と、企業の是正アプローチ (つまり、受け入れる、軽減する、または排除する) と、どのように問題が発生するかに関する詳細会社はすでに対応済み、または今後対応する予定です。

TOPCERTIFIER
www.topcertifier.com

SOC 実装ロードマップ

各 SOC レポートには異なる要件と目的がありますが、通常はそれぞれが実行されます。次の 7 つの主要な段階

プロセス段階		主要な参加者	主要なマテリアル
1	スコーピング	経営トップ 監査役、監査役、監査役	組織の背景 ニーズと顧客の要件
2	ウォークスルーと制御設計	コンサルタント、プロセスオーナー	各プロセス所有者と過ごした時間から
3	ギャップ評価	コンサルタント、プロセスオーナー	予備文書への サポート修復ロードマップ
4	修復	コンサルタント、プロセスオーナー	を検証するための文書 制御環境
5	試験試験	監査人、コンサルタント、プロセス所有者	プロセス文書、検査証拠
6	報告	公認会計士監査役	ポリシーと手順、フィードバック草案、 フィードバックと例外への対応
7	発行	公認会計士監査役	SOCレポート

1 年目の試験であっても、ほとんどの段階は定められた期間内に達成できます。タイムラインは、段階の中で最も予測不可能ですが、修復 (段階 4) です。修復に費やす労力のレベルは、ギャップの結果に基づいて決定されます。評価（ステージ 3）。評価段階で、監査会社は是正措置を提供します。 該当する SOC 基準への準拠を確保するためのロードマップ。強力なコントロールを作成することで、 試験開始前の環境を整えることで、試験の基礎を整えることになります。 組織的で混乱を最小限に抑えた監査。

TOPCERTIFIER
www.topcertifier.com

SOC監査サービス

当社の経験豊富なチームは、AICPA SOC レポート要件についてサービス組織にアドバイスします。私たちは、顧客、見込み客、監査人が評価するために必要な貴重な情報を提供します。アウトソーシングされたサービスプロバイダーに関連するリスクと内部統制。

この分野で適格なコンサルティング会社として、私たちは次の点について数え切れないほどの会話をしてきました。教育、価値、効率性。私たちは、特定の目的を持った組織と協力することに誇りを持っています。ニーズ、競合する優先事項、時間の制約、その他の固有の目的。私たちはそれを理解していますスムーズな試験を確保するための時間の価値、適切な計画、教育 進歩します。

TOPCertifierについて

TOPCertifier は情報に特化した世界的に認められた経営コンサルティング会社です
セキュリティ サービスと社会評価。

バンガロール (インド) に本社を置き、特別なサービスを提供して 20 か国以上で事業を展開しています。米国、ヨーロッパ、湾岸諸国に焦点を当てます。当社はアジアでも印象的な存在感を示しています。太平洋地域とアフリカ地域。私たちはこれまでに 2,800 以上の組織にアドバイスしてきました。 創業以来、会計、税務、収益性、ビジネス プロセス ソリューションに関する業界の専門知識を提供してきました。 2010 年 1 月に。200 名を超える業界専門コンサルタント、認定主任監査人、および 対象分野の専門家の皆様、当社は認定に関して 100% の実績を誇っています。 成功率。

ありがとう

さらに詳しく知りたい場合は、

訪問 WWW.TOPCERTIFIER.COM

TOPCERTIFIER
www.topcertifier.com