



MÉTHODOLOGIE DE SERVICE POUR LA Certification SOC

CONTRÔLE DE L'ORGANISATION DES SERVICES

Que sont les rapports SOC ?



Les rapports SOC sont un moyen pour les entreprises de vérifier, via une assurance tierce indépendante, que les prestataires de services disposent de contrôles appropriés et respectent les normes de l'industrie avant externaliser une fonction commerciale à cette organisation. Cela donne aux prestataires de services la possibilité pour établir la crédibilité et renforcer la confiance auprès des clients, des investisseurs, des partenaires commerciaux et des auditeurs tout en bénéficiant d'un avantage concurrentiel sur le marché. Tous les examens SOC sont effectués selon

Lignes directrices de l'AICPA :

Pendant le processus de mise en œuvre du **SOC**, une équipe expérimentée de consultants en technologie et les auditeurs travailleront en étroite collaboration avec la direction de votre organisation pour garantir que :

- Le rapport SOC final est adapté de manière approfondie et opportune aux besoins uniques d'une organisation
- Les opérations commerciales et les processus de contrôle interne sont rationalisés
- Les obligations contractuelles et les préoccupations du marché sont respectées
- Les exigences de déclaration de l'AICPA sont respectées

Comment déterminer le type de rapport SOC Mes besoins professionnels ?



Il y a deux raisons principales de se soumettre à une évaluation et une certification SOC :

- Un client, un client potentiel ou un auditeur demande un rapport SOC
- Votre organisation décide d'obtenir de manière proactive la conformité sociale

Dans le premier scénario, le demandeur pourrait probablement spécifier le type de rapport SOC requis. Dans l'un ou l'autre Dans ce scénario, une organisation doit d'abord considérer ses objectifs. Généralement, le résultat souhaité pour tout l'organisation doit démontrer son engagement envers une conception appropriée et un fonctionnement efficace de son environnement de contrôle interne

Tableau de comparaison SOC 1, 2 et 3

Il existe 3 types distincts de rapports SOC : SOC 1, SOC 2 et SOC 3. Chaque rapport varie mais fournit des informations précieuses qui sont nécessaires pour évaluer les risques et les contrôles internes associés avec un prestataire externalisé. Un auditeur tiers indépendant est nécessaire pour examiner et affirmer divers aspects d'une organisation avant de produire le rapport final.

SOC 1	SOC 2	SOC 3
Reportez-vous sur votre interne contrôles liés aux finances informations ou déclarations	Rapport sur vos contrôles internes liés à cinq services de confiance principes : sécurité, disponibilité, intégrité, confidentialité et vie privée	Rapport sur les résultats de SOC 2 de manière adaptée au public
Partagé principalement avec les auditeurs	Partagé principalement avec les clients et parties prenantes	Partagé avec le grand public
Applicable aux entreprises qui traite les finances des informations comme les examens médicaux Traitement des réclamations, Paie Services, sociétés de prêt etc	Applicable à toute entreprise technologique qui concerne le traitement de l'information. Basé sur les produits et les services entreprises	Applicable à tout public entreprise qui a un SOC 2 vérifié et souhaite produire un rapport SOC 3 pour un public plus large

CERTIFICATION SOC1



Un rapport SOC 2 se concentre sur les contrôles de votre organisation pertinents pour la situation financière d'une entité utilisatrice rapport. Il s'agit d'un examen hyper détaillé qui nécessite une compréhension spécialisée de l'industrie et l'environnement de contrôle associé. L'organisation de services précise généralement son les objectifs de contrôle et les activités de contrôle associées en fonction des services spécifiques qu'ils effectuent

Un rapport SOC 1 comprend généralement des contrôles de processus métier impliquant l'exécution. Un SOC1 le rapport comprend généralement des contrôles de processus opérationnels impliquant l'exhaustivité et l'exactitude des transactions, ainsi que les contrôles généraux des technologies de l'information, tels que la sécurité des réseaux et accès logique

Compte tenu de sa portée limitée, un rapport SOC 1 convient mieux aux organisations qui doivent inculquer confiance dans leurs contrôles et leurs garanties sur les données financières de leurs clients. C'est souvent nécessaire lorsque l'entité utilisatrice est cotée en bourse et doit se conformer à SOX 404 ou similaire règlements. Voici quelques exemples :



**Tenue de dossiers
Services**



**Réclamations
médicales
traitement**



Services de paie



Pinjaman Layanan

CERTIFICATION SOC2



Un rapport SOC 2 est destiné aux organisations de services dont les entités utilisatrices ne répondent pas nécessairement contrôles des rapports financiers, permettant aux prestataires de répondre aux besoins d'un éventail plus large de entités utilisateur.

Un examen SOC 2 se concentre principalement sur la manière dont les données sont stockées et protégées, en particulier contrôles liés aux engagements de service et aux exigences du système basés sur les normes de l'AICPA. critères des services de confiance (définis ci-dessous).

- **Sécurité** - Les informations et les systèmes sont protégés contre tout accès non autorisé et toute divulgation. d'informations
- **Disponibilité** - Les informations et les systèmes sont disponibles pour être exploités et utilisés afin de répondre aux exigences de l'entité. objectifs
- **Intégrité du traitement** - Le traitement du système est complet, valide, précis, opportun et autorisé à atteindre les objectifs de l'entité
- **Confidentialité** - Les informations désignées comme confidentielles sont protégées pour répondre aux exigences de l'entité. objectifs
- **Confidentialité** - Les informations personnelles sont collectées, utilisées, conservées, divulguées et éliminées pour répondre les objectifs de l'entité

Les rapports SOC 2 peuvent être utilisés par toute entreprise technologique qui s'intéresse à l'information. traitement. Alors que les rapports SOC 1 et SOC 2 ont tous deux un public restreint, les rapports SOC 2 peut être remis à d'autres parties telles que des clients potentiels, la gestion des fournisseurs professionnels, régulateurs et autres partenaires commerciaux clés.

CERTIFICATION SOC3



Comme SOC 2, les rapports SOC 3 se concentrent sur les contrôles pertinents pour les cinq services de confiance de l'AICPA. catégories. Cependant, contrairement au SOC 2, les rapports SOC 3 sont certifiés et peuvent être rendus publics. disponibles, ce qui en fait des outils précieux pour commercialiser l'efficacité de votre contrôle environnement.

Si vous désirez un rapport SOC 3, votre organisation doit d'abord remplir un rapport SOC 2, Type 2. examen (plus d'informations sur les types de rapports ci-dessous). Les examens SOC 2 et SOC 3 peuvent être effectués sur une ou plusieurs catégories de services de confiance. Les rapports SOC 3 contiennent en grande partie la même chose informations incluses dans les rapports SOC 2, sauf avec une description beaucoup moins détaillée de votre contrôles liés à la conformité et aux opérations. Ils ne comportent pas non plus de contrôle spécifique activités, procédures de test ou résultats détaillés sur l'efficacité opérationnelle.

TYPE 1 contre TYPE 2

Tous les rapports SOC (à l'exception du SOC 3) peuvent être de type 1 ou de type 2. La différence est principalement basé sur la période couverte

- **Rapport de type 1** : Un RAPPORT DE TYPE 1 décrit l'adéquation d'un organisme de services aux conception et mise en œuvre de contrôles à un moment précis
- **Rapport de type 2** : Un RAPPORT DE TYPE 2 garantit que les activités de contrôle définies sont cohérentes fonctionner efficacement sur une période définie qui est généralement de 6 mois à 1 an, ce qui permet d'améliorer les performances opérationnelles

Dans de nombreux cas, une organisation de services commencera par un rapport de type 1 pour définir le contrôle activités, à un moment donné. Une fois les contrôles conçus et mis en œuvre, le type 2 un rapport suivrait. Comme le rapport de type 2 couvre une période (c'est-à-dire 6 ou 12 mois), ce rapport est plus précieux pour les utilisateurs car il garantit que, pendant une période, les contrôles fonctionnaient efficacement. Une organisation engage généralement un cabinet d'audit pour réaliser le rapport de type 2, annuellement.

Comment puis-je me préparer à une évaluation SOC ?



Lorsque vous démarrez votre première évaluation SOC, il est avantageux de travailler avec le tiers sélectionné un consultant comme nous pour effectuer une première évaluation des lacunes, vous permettant de remédier à toutes les lacunes avant le début du processus de reporting SOC. Prendre cette route vous aide à combler l'existant lacunes dans votre système actuel, produisant ainsi un système beaucoup plus conforme et très proche pour répondre aux exigences du SOC. Bien que chaque rapport SOC ait une portée différente, il existe certains domaines d'intervention essentiels à toutes les évaluations SOC. En se concentrant sur les tâches suivantes, un l'organisation peut commencer à préparer ses employés à un environnement de contrôle plus fort et donc une évaluation SOC plus efficace.

DOCUMENTATION

Du point de vue des auditeurs, si ce n'est pas documenté, cela n'existe pas. Bien qu'il puisse y avoir Si des contrôles internes stricts sont en place, les preuves de leur apparition peuvent ne pas être mémorisées. Assurer la documentation est conservée pour prendre en charge tous les contrôles en place (par exemple, approbation des autorisations d'accès, remerciements des salariés, maintien des populations, etc.).

POLITIQUES ET PROCÉDURES DÉFINIES

Pour garantir que toutes les parties concernées comprennent leurs responsabilités pour répondre aux exigences organisationnelles objectifs, s'assurer que les processus et procédures fondamentaux sont documentés. Ceci fournit un ressource permettant aux employés et aux auditeurs de comprendre l'intention de l'organisation dans l'environnement de contrôle. La portée des politiques devrait inclure :

- » Procédures organisationnelles pour répondre aux obligations contractuelles
- » Moyens de respecter les principaux engagements de service et les exigences du système
- » Approche de gestion des risques

L'ÉVALUATION DES RISQUES

Un processus formalisé facilité par une discussion annuelle sur l'évaluation des risques et approuvé par le un conseil d'administration ou une direction exécutive devraient exister. Au lieu d'un risque annuel formel évaluation, une organisation peut également choisir de tenir des réunions trimestrielles pour discuter des changements dans menaces, opérations commerciales, etc., et leur impact sur l'évaluation globale des risques. Le risque L'évaluation doit inclure des niveaux de risque définis (c'est-à-dire menace faible, moyenne et élevée) et les L'approche corrective de l'entreprise (c'est-à-dire accepter, atténuer ou éliminer) avec des détails sur la manière dont le L'entreprise a répondu ou envisage de répondre à l'avenir.

Feuille de route de mise en œuvre du SOC

Bien que chaque rapport SOC ait des exigences et des objectifs différents, chacun est généralement réalisé suivant sept étapes principales

ÉTAPE DU PROCESSUS	PARTICIPANTS CLÉS	MATÉRIAUX CLÉS
1 Cadrage	Direction supérieure Commissaires aux comptes, Consultant	Contexte organisationnel besoins et exigences des clients
2 Procédure pas à pas et Conception des contrôles	Consultant , Propriétaires de Processus	Kebijakan dan prosedur yang ada, materi dari waktu yang dihabiskan dengan masing-masing pemilik proses
3 Penilaian Kesenjangan	Consultant , Propriétaires de Processus	Documentation préliminaire à prendre en charge la feuille de route de remédiation
4 Assainissement	Consultant , Propriétaires de Processus	Documentation pour la validation du environnement de contrôle
5 Tests d'examen	Auditeur, Consultant, Processus Propriétaires	Documentation du processus, preuve d'examen
6 Rapport	CPA auditeurs	Politiques et procédures, rédaction de commentaires, réponse aux commentaires et exceptions
7 Émission	CPA auditeurs	Rapport SOC

Même avec les examens de première année, la plupart des étapes peuvent être franchies dans un délai défini. La chronologie, bien que la plus imprévisible des étapes, est celle de la remédiation (étape 4). Le niveau d'effort consacré à la remédiation est déterminé en fonction des résultats de l'écart. évaluation (étape 3). Lors de la phase d'évaluation, votre cabinet d'audit proposera une remédiation feuille de route pour garantir le respect des critères SOC applicables. En créant un contrôle fort environnement avant le début de l'examen, vous posez les bases d'un audit organisé et peu perturbateur.

Services d'audit SOC



Notre équipe expérimentée conseille les organisations de services sur les exigences de reporting AICPA SOC. Nous fournissons des informations précieuses dont les clients, les prospects et les auditeurs ont besoin pour évaluer les risques et les contrôles internes associés à un prestataire de services externalisé.

En tant que cabinet de conseil qualifié dans ce domaine, nous avons eu d'innombrables conversations autour éducation, valeur et efficacité. Nous sommes fiers de travailler avec des organisations qui ont des besoins, priorités concurrentes, contraintes de temps et autres objectifs uniques. Nous comprenons la valeur du temps, une planification appropriée et une formation qui garantissent un examen en toute transparence progresse.

À propos de TOPCertifier

TOPCertifier est un cabinet de conseil en gestion mondialement reconnu, spécialisé dans l'information services de sécurité et évaluations sociales.

Basés à Bangalore (Inde), nous sommes présents dans plus de 20 pays avec un se concentrer sur les États-Unis, l'Europe et les pays du Golfe. Nous avons également une présence impressionnante en Asie Régions Pacifique et Afrique. Nous avons conseillé plus de 2800 organisations, couvrant de nombreux industries, sur les solutions de comptabilité, de fiscalité, de rentabilité et de processus d'affaires, depuis notre création en janvier 2010. Avec une équipe de plus de 200 consultants experts du secteur, auditeurs principaux certifiés et Experts en la matière, nous avons fourni un historique de 100 % en termes de notre certification taux de réussite.



Merci

**POUR EN SAVOIR PLUS,
VISITE WWW.TOPCERTIFIER.COM**