



METODOLOGIA DEL SERVIZIO PER la certificazione SOC

CONTROLLO DELL'ORGANIZZAZIONE DEI SERVIZI

Cosa sono i report SOC?



Rapporti del SOC sono un modo per le aziende di verificarlo tramite una garanzia di terze parti indipendenti i fornitori di servizi dispongono già di controlli adeguati e seguono gli standard del settore esternalizzare una funzione aziendale a tale organizzazione. Ciò offre ai fornitori di servizi un'opportunità per stabilire credibilità e creare fiducia con clienti, investitori, partner commerciali e revisori dei conti ottenendo allo stesso tempo un vantaggio competitivo sul mercato. Vengono eseguiti tutti gli esami SOC come da

Linee guida AICPA:

Durante il processo di **Implementazione del SOC** un team esperto di consulenti tecnologici e i revisori lavoreranno a stretto contatto con la leadership della vostra organizzazione per garantire che:

- Il report SOC finale è personalizzato in modo accurato e tempestivo in base alle esigenze specifiche di un'organizzazione
- Le operazioni aziendali e i processi di controllo interno sono semplificati
- Gli obblighi contrattuali e le preoccupazioni del mercato vengono rispettati
- I requisiti di rendicontazione AICPA sono soddisfatti

Come posso determinare il tipo di rapporto SOC Le mie esigenze aziendali?



Esistono due motivi principali per sottoporsi a una valutazione e certificazione SOC:

- Un cliente o potenziale cliente o un revisore richiede un rapporto SOC
- La tua organizzazione decide di ottenere in modo proattivo la conformità SOC

Nel primo scenario, il richiedente potrebbe probabilmente specificare il tipo di report SOC necessario. In entrambi i casi scenario, un'organizzazione deve prima considerare i propri obiettivi. In genere, il risultato desiderato per any L'organizzazione deve dimostrare il proprio impegno per una progettazione appropriata e un funzionamento efficace del suo ambiente di controllo interno.

Tabella comparativa SOC 1, 2 e 3

Esistono 3 tipi distinti di report SOC: SOC 1, SOC 2 e SOC 3. Ciascun report varia ma fornisce informazioni preziose necessarie per valutare i rischi e i controlli interni associati con un fornitore di servizi in outsourcing. Per l'esame è necessario un revisore indipendente di terze parti affermare vari aspetti di un'organizzazione prima di produrre il rapporto finale.

SOC 1	SOC 2	SOC 3
Riporta il tuo interno controlli relativi agli aspetti finanziari informazioni o dichiarazioni	Riporta i tuoi controlli interni relativi a cinque servizi fiduciari principi: sicurezza, disponibilità, integrità, riservatezza e privacy	Rapporto sui risultati di SOC 2 in modo adeguato al pubblico pubblico
Condiviso principalmente con i revisori dei conti	Condiviso principalmente con clienti e parti interessate	Condiviso al grande pubblico
Applicabile alle aziende quale processo finanziario informazioni come le visite mediche Elaborazione sinistri, buste paga Servizi, Società di Credito ecc	Applicabile a qualsiasi azienda tecnologica che si occupa dell'elaborazione delle informazioni. Basato sia sul prodotto che sul servizio aziende	Applicabile a qualsiasi pubblico impresa che ha a SOC 2 verificato e desiderato per produrre un rapporto SOC 3 per un pubblico più vasto

CERTIFICAZIONE SOC 1



Un report SOC 2 si concentra sui controlli della tua organizzazione rilevanti per le finanze di un'entità utente segnalazione. È un esame iper-dettagliato che richiede una comprensione specializzata del settore e relativo ambiente di controllo. L'organizzazione del servizio in genere specifica la propria obiettivi di controllo e relative attività di controllo in base agli specifici servizi prestati.

Un report SOC 1 generalmente include i controlli dei processi aziendali che coinvolgono la prestazione. Un SOC1 il rapporto generalmente include controlli dei processi aziendali che riguardano la completezza e l'accuratezza del rapporto transazioni, nonché controlli generali sulla tecnologia dell'informazione, come la sicurezza della rete e accesso logico.

Dato l'ambito limitato, un report SOC 1 è più adatto per le organizzazioni che devono infondere fiducia nei controlli e nelle garanzie sui dati finanziari dei propri clienti. Lo è spesso necessario quando l'entità utente è quotata in borsa e deve rispettare SOX 404 o simili regolamenti. Ecco alcuni esempi:



**Tenuta dei registri
Servizi**



**Affermazioni
mediche
elaborazione**



Servizi di buste paga



Servizi di prestito

CERTIFICAZIONE SOC 2



Un report SOC 2 è destinato alle organizzazioni di servizi le cui entità utente non necessariamente rispondono controlli per la rendicontazione finanziaria, consentendo ai fornitori di soddisfare le esigenze di una gamma più ampia di entità utente.

Un esame SOC 2 si concentra principalmente sul modo in cui i dati vengono archiviati e protetti, in particolare controlli relativi agli impegni di servizio e ai requisiti di sistema basati sull'AICPA criteri relativi ai servizi fiduciari (definiti di seguito).

- **Sicurezza** – Le informazioni e i sistemi sono protetti contro l'accesso e la divulgazione non autorizzati di informazioni
- **Disponibilità** – Le informazioni e i sistemi sono disponibili per il funzionamento e l'utilizzo per soddisfare le esigenze dell'entità obiettivi
- **Integrità dell'elaborazione** – L'elaborazione del sistema è completa, valida, accurata, tempestiva e autorizzato a raggiungere gli obiettivi dell'entità
- **Riservatezza** – Le informazioni designate come riservate sono protette per soddisfare le esigenze dell'entità obiettivi
- **Privacy** – Le informazioni personali vengono raccolte, utilizzate, conservate, divulgate e smaltite per soddisfare gli obiettivi dell'entità

I rapporti SOC 2 possono essere utilizzati da qualsiasi azienda tecnologica interessata all'informazione elaborazione. Mentre i report SOC 1 e SOC 2 hanno entrambi un pubblico limitato, i report SOC 2 possono essere forniti ad altre parti come potenziali clienti, gestione del fornitore professionisti, regolatori e altri partner commerciali chiave.

CERTIFICAZIONE SOC 3



Come SOC 2, i rapporti SOC 3 si concentrano sui controlli rilevanti per i cinque servizi fiduciari dell'AICPA categorie. Tuttavia, a differenza del SOC 2, i report SOC 3 sono certificati e possono essere resi pubblici disponibili, rendendoli strumenti preziosi per commercializzare l'efficacia del tuo controllo ambiente.

Se desideri un report SOC 3, la tua organizzazione deve prima completare un SOC 2, Tipo 2 esame (maggiori informazioni sui tipi di report di seguito). È possibile eseguire gli esami SOC 2 e SOC 3 su una o più categorie di servizi fiduciari. I rapporti SOC 3 contengono più o meno la stessa cosa informazioni incluse nei rapporti SOC 2, ad eccezione di una descrizione molto meno dettagliata del tuo controlli relativi alla conformità e alle operazioni. Inoltre non includono un controllo specifico attività, procedure di test o risultati dettagliati sull'efficacia operativa.

TIPO 1 contro TIPO 2

Tutti i report SOC (eccetto SOC 3) possono essere di Tipo 1 o di Tipo 2. La differenza è principalmente in base al periodo in esame

- **Rapporto di tipo 1** : AUN RAPPORTO DI TIPO 1 descrive l'idoneità di un'organizzazione di servizi progettazione e implementazione dei controlli in un determinato momento
- **Rapporto di tipo 2** : UN RAPPORTO DI TIPO 2 garantisce che le attività di controllo definite siano coerenti operare in modo efficace per un periodo definito che di solito va da 6 mesi a 1 anno, ottenendo così migliori prestazioni operative

In molti casi, un'impresa di servizi inizierà con un report di Tipo 1 per definire il controllo attività, in un determinato momento. Una volta progettati e implementati i controlli, il Tipo 2 i sarebbe seguito il rapporto. Poiché il rapporto di tipo 2 copre un periodo (ovvero 6 o 12 mesi), questo rapporto è più prezioso per gli utenti perché garantisce che, durante un periodo, i controlli fossero operativi in modo efficace. Un'organizzazione in genere incarica una società di revisione di completare il rapporto di tipo 2, annualmente.

Come mi preparo per una valutazione SOC?



Quando inizi la tua prima valutazione SOC, è utile collaborare con la terza parte selezionata un consulente come noi per eseguire una valutazione iniziale delle lacune, consentendoti di colmare eventuali lacune prima dell'inizio del processo di reporting del SOC. Intraprendere questo percorso aiuta a riempire l'esistente lacune nel vostro sistema attuale, producendo così un sistema molto più conforme e molto vicino per soddisfare i requisiti del SOC. Sebbene ogni rapporto SOC abbia una portata diversa, ce ne sono alcuni aree di interesse essenziali per tutte le valutazioni SOC. Concentrandosi sui seguenti compiti, an l'organizzazione può iniziare a preparare i propri dipendenti per un ambiente di controllo più forte e quindi una valutazione SOC più efficiente.

DOCUMENTAZIONE

Dal punto di vista degli auditor, se non è documentato allora non esiste. Anche se potrebbe essere forti controlli interni in atto, la prova dell'evento potrebbe non essere commemorata. Garantire viene conservata la documentazione per supportare tutti i controlli in atto (ad esempio, approvazione per le concessioni di accesso, riconoscimenti dei dipendenti, mantenimento delle popolazioni, ecc.).

POLITICHE E PROCEDURE DEFINITE

Per garantire che tutte le parti interessate comprendano le proprie responsabilità per soddisfare le esigenze organizzative obiettivi, garantire che i processi e le procedure fondamentali siano documentati. Ciò fornisce a risorsa sia per i dipendenti che per i revisori per comprendere le intenzioni dell'organizzazione al suo interno l'ambiente di controllo. L'ambito delle politiche dovrebbe includere:

- » Procedure organizzative per far fronte agli obblighi contrattuali
- » Mezzi per soddisfare i principali impegni di servizio e i requisiti di sistema
- » Approccio alla gestione del rischio

VALUTAZIONE DEL RISCHIO

Un processo formalizzato facilitato da una discussione annuale sulla valutazione del rischio e approvato dal dovrebbe esistere un consiglio di amministrazione o una direzione esecutiva. Al posto di un rischio annuale formale valutazione, un'organizzazione può anche decidere di tenere riunioni trimestrali per discutere i cambiamenti minacce, operazioni aziendali, ecc. e il loro impatto sulla valutazione complessiva del rischio. Il rischio la valutazione dovrebbe includere livelli di rischio definiti (vale a dire, minaccia bassa, media e alta) e l'approccio correttivo dell'azienda (ovvero accettare, mitigare o eliminare) con dettagli su come L'azienda ha risposto o prevede di rispondere in futuro.

Roadmap di implementazione del SOC

Sebbene ogni report SOC abbia requisiti e obiettivi diversi, generalmente viene eseguito ciascuno seguendo sette fasi principali

FASE DEL PROCESSO		PARTECIPANTI CHIAVE	MATERIALI CHIAVE
1	Ambito	Alta direzione Revisori dei Conti, Consulente	Background organizzativo esigenze e richieste del cliente
2	Procedura dettagliata e Progettazione del controllo	Consulente, Process Owner	Politiche e procedure esistenti, materiali dal tempo trascorso con ciascun proprietario del processo
3	Valutazione delle lacune	Consulente, Process Owner	Documentazione preliminare a sostenere la tabella di marcia di riparazione
4	Bonifica	Consulente, Process Owner	Documentazione per la validazione del ambiente di controllo
5	Prove d'esame	Revisore, Consulente, Processo Proprietari	Documentazione del processo, prove dell'esame
6	Rapporto	Revisori dei conti CPA	Politiche e procedure, bozza di feedback, risposta al feedback e alle eccezioni
7	Emissione	Revisori dei conti CPA	Rapporto SOC

Anche con gli esami del primo anno, la maggior parte delle fasi può essere completata entro un tempo definito la sequenza temporale, sebbene la più imprevedibile delle fasi, è la riparazione (fase 4). Il livello di sforzo speso per la riparazione è determinato in base ai risultati del divario valutazione (fase 3). Durante la fase di valutazione, la vostra società di revisione fornirà una soluzione correttiva tabella di marcia per garantire la conformità ai criteri SOC applicabili. Creando un forte controllo ambiente prima dell'inizio dell'esame, stai gettando le basi per un audit organizzato e con interruzioni minime.

Servizi di verifica SOC



Il nostro team esperto fornisce consulenza alle organizzazioni di servizi sui requisiti di reporting del SOC AICPA. Forniamo informazioni preziose che i clienti, i potenziali clienti e i revisori richiedono di valutare i rischi e i controlli interni associati a un fornitore di servizi esternalizzati.

In quanto società di consulenza qualificata in questo ambito, abbiamo avuto innumerevoli conversazioni in giro istruzione, valore ed efficienza. Siamo orgogliosi di lavorare con organizzazioni che hanno specifiche esigenze, priorità concorrenti, vincoli di tempo e altri obiettivi unici. Comprendiamo il valore del tempo, pianificazione adeguata e formazione che garantiscano un esame senza intoppi progredisce.

Informazioni su TOPCertifier

TOPCertifier è una società di consulenza gestionale riconosciuta a livello mondiale specializzata in informazioni servizi di sicurezza e valutazioni soc.

Con sede a Bangalore (India), operiamo in oltre 20 paesi con uno speciale focus su USA, Europa e Paesi del Golfo. Abbiamo anche una presenza impressionante in Asia-Regioni del Pacifico e dell'Africa. Abbiamo fornito consulenza a oltre 2.800 organizzazioni, tra cui numerose fin dall'inizio, su soluzioni contabili, fiscali, di redditività e di processi aziendali nel gennaio 2010. Con un team di oltre 200 consulenti esperti del settore, lead auditor certificati e Esperti in materia, abbiamo fornito un track record del 100% in termini di certificazione tasso di successo.



Grazie

**PER SAPERNE DI PIÙ,
VISITA WWW.TOPCERTIFIER.COM**