Vision Pro n. 21/2018

Gli *standards* per la *compliance* del sistema di controllo interno della *service organization*: *SOC reports*

di Tiziana Guggino – dottore commercialista e revisore legale in Pisa e CPA abilitato all'attestazione dei sistemi di controllo interno

I mercati in continua evoluzione, l'importanza dell'organizzazione e l'esigenza di tutelare i risparmiatori rispetto alle informazioni contenute nel financial reporting hanno dato luogo all'emanazione, nel tempo, da parte degli organismi internazionali dei certificatori pubblici contabili (Aicpa, Iaasb, Ifac), di linee guida e standards di controllo che definiscono i requisiti del sistema di controllo interno cui gli studi professionali e, in generale, le Service Organizations devono uniformarsi. Sulla gestione del rischio (risk management), attività di primaria importanza per qualsiasi tipo di organizzazione, si sono concentrati ultimamente, ritenendola una questione focale, anche gli organismi internazionali che hanno provveduto a regolamentare sia la Privacy (Regolamento UE 679/2016 – GDPR), sia il Sistema di gestione qualità Iso 9001:2015.

In un mercato in continua evoluzione, gli studi commercialisti e di consulenza del lavoro, i Ced e, in generale, le aziende di servizi mostrano una crescente attenzione verso le "certificazioni" internazionali che rappresentano, oggi ancora più di ieri, requisiti fondamentali per poter approdare sui mercati internazionali. In realtà, più che di certificazioni, dovremmo parlare di *standards*, ossia di attestazioni di conformità o *compliance*.

In qualsiasi azienda o studio professionale si rivela di cruciale importanza la sua organizzazione che deve essere strutturata al fine dell'erogazione di un buon servizio, ma anche per ottenere efficienze nell'organizzazione medesima, sia dal punto di vista economico, sia del tempo impiegato per l'erogazione del servizio stesso.

Gli *standards* che nell'era attuale impattano maggiormente sull'organizzazione in quanto considerati spesso requisiti fondamentali e imprescindibili per il mantenimento di clienti esistenti e l'acquisizione di nuovi clienti sono l'Ssae 18 e l'Isae 3402.

Spesso sono i clienti a richiedere allo studio o al Ced di dotarsi di una certificazione rispetto a determinati *standards* internazionali. Ciò accade in speciale modo per le aziende appartenenti a gruppi

internazionali le cui capogruppo siano ad esempio quotate in borsa negli Stati Uniti o in altri Paesi. Nulla vieta, tuttavia, che gli studi professionali, i Ced e le aziende che erogano servizi si dotino di queste attestazioni anche per motivazioni di miglioramento dei propri processi o della propria immagine esterna, analogamente ad altri *standards* quali la Iso 9001. Un ulteriore motivo di adesione agli *standards* potrebbe essere legato al posizionamento, cioè al desiderio di acquisire clientela di caratura internazionale.

Gli *standards* stabiliscono generalmente una serie più o meno stringente di requisiti di organizzazione e documentazione delle responsabilità, dei processi e dei controlli che vengono svolti all'interno dell'impresa o studio che agisce come *outsourcer*. La struttura organizzativa viene resa conforme dal *management*, durante il periodo sottoposto a revisione, con il supporto dell'*auditor indipendente* il quale, alla fine del periodo, rilascia il *report* di conformità.

Prima di descrivere gli *standards* che riguardano l'organizzazione degli studi professionali e delle aziende che erogano servizi in *outsourcing*, però, occorre necessariamente fare un salto indietro nel tempo e tornare alle origini degli stessi che rappresentano, al giorno d'oggi, un segno distintivo delle realtà aziendali e professionali rispetto ai propri *competitors*.

La nascita degli *standards* di controllo interno estesi agli *outsourcers*

A causa dello scandalo del colosso energetico Enron, che nel 2002 provocò ingenti danni finanziari agli investitori, fu emanato dal Governo degli Stati Uniti il Sarbanes Oxley Act (SOX) che, nella sezione 404, stabilì l'obbligo di attestazione, da parte del *management* delle aziende quotate in borsa, dell'osservanza dei rigorosi controlli previsti dalla legge medesima circa il sistema di controllo interno dell'organizzazione aziendale. Ciò, allo scopo di tutelare i terzi riguardo la veridicità delle informazioni scaturenti dal *Financial Reporting*, cioè dal bilancio finanziario. Infatti, i risparmiatori, cioè gli azionisti di una società quotata in borsa, al fine di investire i propri risparmi mediante l'acquisto di azioni, prendono le loro decisioni in base al bilancio finanziario e, se questo non è veritiero, rischiano di perdere i propri risparmi, come appunto accadde agli azionisti dell'Enron. La sezione 404 del Sarbanes Oxley Act stabilisce anche che il Ceo (*Chief Executive Officer*) e il Cfo (*Chief Financial Officer*) devono attestare di aver osservato, durante l'esercizio delle proprie funzioni, i rigidi controlli prescritti dalla Legge medesima.

A seguito delle richieste della norma suddetta, si è sempre più diffuso l'utilizzo del Sas 70, "*Statement on Auditing Standard*" No. 70, emanato dall'Aicpa (*American Institute of Certified Public Accountants*), nel 1992, che sancisce le linee guida e le regole per l'emissione di un'opinione indipendente, da parte di

un revisore di servizio (*service auditor*) abilitato, sui servizi forniti da parte di un *service provider* (o *service outsourcer*) ai propri clienti. L'opinione indipendente sul sistema di controllo interno dell'organizzazione di servizi viene espressa attraverso un *report* - che è il risultato dell'attività di *auditing* svolta in conformità allo *standard* Sas 70 - rilasciato dal revisore del servizio al *service provider* medesimo. Ricordiamo che l'Aicpa è l'organismo regolatore della professione di commercialista negli Stati Uniti.

Il Sas 70 assicura che il fornitore di servizi (*service outsourcer*) abbia superato i più rigidi *test* delle terze parti e che si attenga ai rigorosi processi interni per quel che riguarda la sicurezza, lo sviluppo degli applicativi, le comunicazioni, il servizio ai clienti e la pianificazione di eventi imprevisti e che ottemperi ad altri requisiti obbligatori imposti dal Sarbanes-Oxley Act.

Ma vediamo chi sono i soggetti coinvolti nello *standard*:

Il *service provider* (o *service outsourcer*) è l'azienda che fornisce servizi o svolge importanti parti del processo del cliente. Un esempio è l'azienda che offre un Sas (*software as a service*), un *internet data center*, un servizio di elaborazione paghe e contributi e/o amministrativo-contabile, un centro per il processamento di transazioni bancarie, di gestione elettronica dei documenti, etc..

Il *service auditor* è l'*auditor indipendente* che ha il compito di controllare, a sua volta, i controlli eseguiti dal *service provider* sul proprio sistema di controllo interno (Sci) in base allo *standard* suddetto ed esprimere un'opinione attraverso il rilascio di un report sull'attività di *auditing* svolta sull'organizzazione medesima.

La *user organization* è l'azienda cliente del *service provider*, cioè l'organizzazione che usufruisce del servizio offerto dall'*outsourcer*. Importante è quest'ultima figura che entra, in modo incisivo, nelle scelte del *service outsourcer* riguardo la *compliance* allo *standard* di riferimento.

Questi 3 soggetti interagiscono tra loro a salvaguardia dei dati che formano il *financial reporting* e quindi degli investitori.

L'evoluzione dello *standard* per la *compliance* del Sistema di controllo interno (Sci)

Interessante è l'evoluzione che nel tempo ha subito il Sas 70 migrando all'Ssae 16 e infine all'Ssae 18, ciascuno apportando rilevanti miglioramenti dal punto di vista dei controlli che gli *outsourcers*, indicati semplicemente come *service organizations*, devono obbligatoriamente osservare nel rispetto degli *standards* stessi.

Il Sas 70 è stato superato a partire dal 1° luglio 2011 dall'Ssae 16 (*statement on standards for attestation engagement* no. 16) che ha introdotto alcuni elementi che vanno a rafforzare i controlli già compresi nel primo *standard* e, dal 1° maggio 2017, dall'Ssae 18.

Man mano che si è passati dal Sas 70 all'Ssae 18, attraverso l'emanazione dell'Ssae 16, sono stati introdotti significativi miglioramenti agli *standards* medesimi in tema di obiettivi di controllo del Sci della *service organization*. L'Ssae 16 va oltre i requisiti prescritti dal Sas 70, richiedendo l'*auditor indipendente* di ottenere dal *management* della *service organization* un'affermazione scritta (*management assertion letter*) sulla gestione per quanto concerne l'efficacia dell'implementazione e del funzionamento dei controlli in corso di *auditing*.

Lo *standard* Ssae 16 fornisce, inoltre, un migliore allineamento con il principio internazionale Isae (*International standard for assurance engagements*) 3402 emanato dallo Iaasb (*International auditing and assurance standards board*).

In base alle nuove linee guida dettate dall'Aicpa relativamente agli *standards* di rendicontazione, a partire dal 1° luglio 2011, l'*audit* che si svolge in linea con l'Ssae 16 viene rendicontato in un *System and organization controls* (Soc) 1 *report*. Questo tipo di *report* rimane focalizzato sui controlli rilevanti ai fini del controllo interno sulla rendicontazione finanziaria. Dal 1° maggio 2017 è in vigore l'Ssae 18, un nuovo *standard* emanato dall'Aicpa, comprendente una serie di miglioramenti intesi ad aumentare l'utilità e la qualità dei rapporti Soc, che sostituisce lo *standard* Ssae 16 e, ovviamente, il vecchio rapporto di revisione Sas 70. Le modifiche apportate alla norma richiedono alle aziende di prendere maggior consapevolezza dei propri controlli interni in riferimento all'identificazione e alla classificazione del rischio e all'adeguata gestione dei rapporti con le organizzazioni subappaltanti.

Questi cambiamenti, pur non troppo onerosi, contribuiscono a chiudere il cerchio sui settori chiave in quanto i professionisti del settore hanno notato l'esistenza di lacune in molti *reports* delle organizzazioni di servizi (*service organizations* o *outsourcers*). Tutte le organizzazioni di servizi sono ora obbligate a pubblicare la valutazione relativa ai controlli del sistema e dell'organizzazione (Soc – *System and organization controls*) sotto lo *standard* Ssae 18 in un *report* Soc 1. La relazione Soc 1, rilasciata da un *auditor indipendente*, appare molto simile a quella rilasciata a livello di Ssae 16, ma si distingue da quest'ultima in quanto contiene un paio di sezioni aggiuntive e i controlli necessari a migliorarne ulteriormente il contenuto e la qualità e, quindi, la capacità di affidarsi a terzi.

Isae 3402

Uno *standard* molto simile all'Ssae 16 di matrice nordamericana è l'Isae 3402 (*International standard for assurance engagements* no. 3402) un principio emanato nel giugno 2011 da Iaasb (*International auditing*

and assurance standards board), organo dell'Ifac (*international federation of accountants*) e riconosciuto a livello internazionale. Anch'esso, come l'Ssae 16 è un Soc 1. Il *report* Isae 3402, come peraltro l'Ssae 16, consiste nella valutazione del sistema dei controlli di organizzazioni che erogano servizi, prevalentemente in ambito IT e *payroll*, ed è rilasciato da *auditors* indipendenti responsabili di valutarne la descrizione, il disegno e l'efficacia, rispetto a *best practices* di controllo (ad esempio Cobit, cioè il *framework* per la *governance* e il *controllo* IT).

Il *report* è emesso per essere utilizzato dalle società che utilizzano i servizi oggetto di verifica e dei loro rispettivi *auditors*, in quanto tali servizi supportano la produzione dell'informativa contabile e di bilancio.

Ricordiamo che l'Ifac (*International federation of accountants*) è l'organizzazione globale per la professione contabile dedicata a servire l'interesse pubblico rafforzando la stessa e contribuendo allo sviluppo di forti economie internazionali e che Aicpa e Iaasb operano sotto la sua tutela al pari del Cndcec.

Rammentiamo che lo *standard* Isae 3402 è stato tradotto in italiano dal Cndcec ed è disponibile gratuitamente per la consultazione sul sito www.commercialisti.it.

Secondo l'orientamento attuale più diffuso, gli studi professionali e le aziende interessate tendono solitamente a dotarsi di entrambi i *reports,* americano e internazionale, per rispondere contemporaneamente alle richieste delle *user organizations* americane ed europee.

Ssae 18

L'Ssae 18 (*Statement on standards for attestation engagement* n. 18), di Aicpa, come i princìpi che l'hanno preceduto, non è altro che una dichiarazione sugli *standards* per l'attestazione dell'impegno n. 18. In pratica, si tratta di un'*opinion*, rilasciata sotto forma di *report* da parte di un *auditor indipendente* abilitato, sul sistema di controllo interno implementato da un'organizzazione che offre servizi in *outsourcing* (*service organization*).

Che cosa c'è di nuovo in Ssae 18 rispetto a Ssae 16?

Con la migrazione dall'Ssae 16 all'Ssae 18, le aziende che attualmente eseguono un Soc 1, devono prendere in considerazione di attuare:

– un programma formale di gestione delle organizzazioni subappaltanti intese come le organizzazioni utilizzate dalla *service organization* per eseguire alcuni dei servizi forniti alle entità utenti che sono probabilmente rilevanti per il controllo interno sul rendiconto finanziario;

– un processo formale annuale di valutazione dei rischi (*risk analysis*).

Per le aziende che non sono state precedentemente sottoposte a un *audit* Soc 1, poiché i loro servizi non erano finanziariamente significativi, Ssae 18 ora amplia la definizione di ciò che è consentito inserire nella relazione al fine di mettere in *compliance* un'impresa rispetto a determinate leggi o regolamenti, accordi contrattuali o a un altro insieme di procedure concordate e definite, riguardo a un servizio in *outsourcing* in cui la convalida di terze parti dovrebbe essere vantaggiosa e aggiungere sicurezza. Grazie a questo ampliamento, ora è possibile permettere una revisione ufficiale e indipendente di un'ampia gamma di operazioni in un insieme di linee guida relative ad *audit* e a *reporting* attendibili e coerenti.

Chi necessita di un *audit* Ssae 18/Isae 3402 (Soc 1)?

I servizi forniti da una *service organization* fanno parte del sistema informativo di un'entità (impresa o *user organization*) se interessano una delle seguenti caratteristiche:

– le classi di transazioni nelle operazioni dell'impresa che sono significative dal punto di vista finanziario per i bilanci dell'impresa stessa;

– le procedure, sia automatiche sia manuali, con le quali le operazioni dell'impresa vengono effettuate tenuto conto dell'intero ciclo di vita fino alla loro inclusione nel bilancio;

– le relative registrazioni contabili, le informazioni di supporto e i conti specifici nei bilanci finanziari dell'impresa;

– la modalità secondo cui il sistema di informazione dell'impresa acquisisce altri eventi e condizioni significativi per il bilancio;

– il processo di rendicontazione finanziaria utilizzato per la redazione dei bilanci dell'impresa, comprese stime contabili e divulgazioni significative.

Se la *service organization* eroga servizi esternalizzati (in *outsourcing*) che incidono sui rendiconti finanziari di un'altra società (la c.d. organizzazione utente), è più che probabile che le sia richiesto di fornire un *report* Soc 1 *type* II, specialmente se la *user organization* è quotata in Borsa. Generalmente, gli *outsourcers* cui il *report* Soc 1 viene richiesto sono aziende i cui servizi erogati incidono significativamente sul *financial reporting* della *user organization* come, ad esempio le aziende che elaborano cedolini paghe, aziende di informatica, gestione documentale, studi amministrativo-contabili.

Chi richiede un Soc 1?

Il report Soc 1 viene richiesto perché il Ceo o Cfo di una *user organization* si assume in proprio la responsabilità dei dati forniti dall'*outsourcer*, laddove questi incide materialmente e qualitativamente nei dati di bilancio da indirizzare nel *financial reporting*. Per quanto riguarda l'Ssae 18 *report*, questo viene richiesto, solitamente, dalle aziende clienti della *service organization* che devono assolvere le richieste della sezione 404 del *Sarbanes-Oxley act* al fine di garantire controlli e processi interni appropriati per la gestione delle informazioni dei clienti.

Esistono 2 tipi di *service auditor's reports*

Report type I

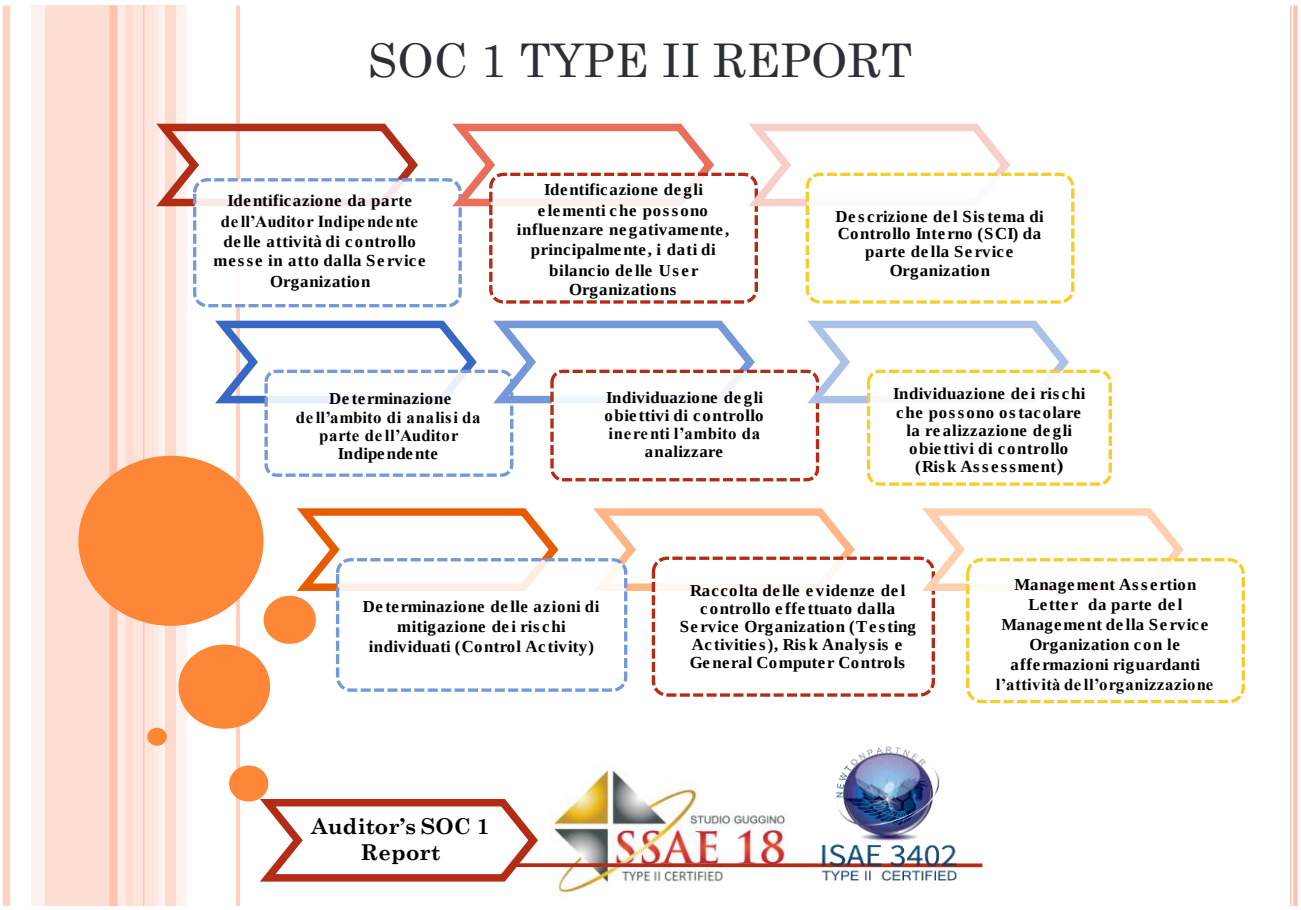
Nel *reports di tipo 1*, (*type I report*), l'*auditor indipendente* (cioè il revisore del servizio) esprime un'opinione su:

1. la rappresentazione imparziale della descrizione dei controlli, in tutti gli aspetti rilevanti dei controlli della *service organization* che sono stati implementati e resi operativi a partire da una specifica data;
2. l'adeguato disegno dei controlli per il raggiungimento degli obiettivi di controllo. Questa tipologia di report è utile per fornire al revisore del cliente della *service organization* la comprensione dei controlli necessari a pianificare il proprio *audit* sul cliente, disegnare i *test* ed eseguirli in maniera indipendente.

Report type II

Nel *report di tipo 2*, (*type II report*) l'*auditor indipendente* esprime un'opinione, oltre che sugli stessi argomenti del *type I report*, anche sul fatto che i controlli verificati presentino un sufficiente livello di efficacia per fornire una ragionevole, ma non assoluta, confidenza che gli obiettivi di controllo siacno stati assolti in un determinato periodo di tempo. Si contraddistingue, quindi, dal *type I* perché esprime un'*opinion* sull'efficacia dei controlli, di conseguenza, per ridurre al minimo il numero di visite da parte dei revisori delle entità utenti - in particolare se l'organizzazione del servizio dispone di un numero elevato di entità utente - è preferibile che essa si doti di un report di tipo 2.

L'*iter* per la *compliance agli standards*



Vantaggi

L'adesione agli *standards* internazionali di controllo interno porta a rilevanti vantaggi sia per la *service organization* (lo studio professionale, il Ced, l'azienda di servizi), sia per la *user organization* (l'azienda committente).

Per la *service organization*:

– maggiore efficienza organizzativa nei tempi di esecuzione dei servizi e della risoluzione dei problemi con conseguente riduzione dei costi aziendali;

– riduzione degli errori;

– miglioramento dell'immagine dell'azienda sul mercato;

– maggiore competitività sui mercati internazionali;

– possibilità di partecipazione alle gare di appalto pubbliche e private dove sia richiesto il requisito della *compliance* a uno di questi *standards*.

Per la user organization:

– servizio garantito da controlli certificati;

– riduzione dei costi associati alle attività interne di revisione del bilancio interne.

Uno sguardo ai Soc 2 e Soc 3

È possibile richiedere all'*auditor* l'emissione di *reports* diversi dal Soc 1. In particolare, i *reports* Soc 2 e 3 forniscono requisiti di controllo molto più rigorosi rispetto a quelli previsti dai *reports* Soc 1 con un insieme di controlli più efficaci e requisiti specificamente progettati intorno ai dati delle organizzazioni utenti e un *benchmark*, ossia un parametro di riferimento, *standard* con il quale 2 *service organizations* soggette a verifiche possono essere confrontate sulla base degli stessi criteri.

Il Soc 2 *report* include molti elementi del Soc 1 *report* e indirizza ai controlli identificati dal *trust services principles and criteria* quali:

– *sicurezza*;

– *disponibilità*;

– *integrità dei processi*;

– *riservatezza*;

– *privacy*.

La sezione AT 101 del *code of professional conduct* di Aicpa, (che definisce i controlli del Soc 2 *report*) svolgerà un ruolo fondamentale nella segnalazione dei controlli presso le *service organizations* a causa del numero ampio e in costante crescita di entità nei settori "*cloud computing*" e tecnologia attuali. Le organizzazioni che forniscono *Software* as a *service* (Saas o Sas), *Infrastructure as a service* (Iaas) servizi gestiti, *cloud computing* e *host* di altri servizi relativi alla tecnologia, molto probabilmente, riceveranno richieste di pubblicazione di *reports* Soc sotto lo *standard* della sezione AT 101.

Il Soc 3 *report* è progettato per soddisfare le esigenze degli utenti che necessitano di garanzie sui controlli presso una *service organization* rilevante *per sicurezza, disponibilità, riservatezza* dell'*integrità* del processo o *privacy*, ma che non ha la necessità o le conoscenze necessarie per utilizzare in modo efficace un Soc 2 *report*. Poiché si tratta di un rapporto di uso generale, il *report* Soc 3 può generalmente essere distribuito liberamente.

Occorre però ricordare che anche nell'Ssae 18 *report* viene testata la *compliance* dei controlli eseguiti dalla *service organization* in termini di *sicurezza, disponibilità, integrità dei processi, riservatezza* e *privacy* legati all'erogazione del servizio anche se non in modo così strettamente dettagliato come negli altri 2 tipi di Soc.