Standard di audit e assurance IS 1205 Evidenza

La natura specialistica dei processi di audit e assurance dei Sistemi Informativi (IS) e le competenze necessarie per svolgere tali incarichi impongono la definizione di standard specifici. Lo sviluppo e la divulgazione degli standard di audit e assurance IS rappresentano il contributo professionale di ISACA® alla comunità dei revisori.

Gli standard di audit e assurance IS definiscono i requisiti obbligatori per i processi di auditing e reporting di natura informatica e rendono edotti:

- i revisori di Sistemi Informativi sul livello minimo di una prestazione, da considerare accettabile, necessario per soddisfare le responsabilità professionali previste dal Codice di etica professionale di ISACA
- la direzione e le altre parti interessate sulle ragionevoli aspettative per quanto attiene tali attività professionali relativamente all'operato degli addetti
- i certificati CISA® (Certified Information Systems Auditor®) sui requisiti per l'accreditamento. La mancata osservanza di tali standard potrebbe sfociare in un'indagine sulla condotta del detentore della certificazione CISA da parte del consiglio direttivo ISACA o del comitato appropriato e, in ultima istanza, in misure disciplinari.

I revisori di Sistemi Informativi sono tenuti a dichiarare, ove appropriato, che l'incarico è stato portato a termine nel rispetto degli standard di audit e assurance di ISACA o di altri standard del settore.

Il framework *ITAF*™ destinato ai revisori di Sistemi Informativi offre più livelli di applicazione:

- **Standard**, divisi in tre categorie:
  - Standard generali (serie 1000): principi guida nel rispetto dei quali deve operare il revisore. Si applicano alla condotta di tutti i lavori assegnati e riguardano l'etica, l'indipendenza, l'oggettività, la dovuta attenzione, nonché le conoscenze e le competenze dei revisori. Il rispetto degli standard definiti (in **grassetto**) è obbligatorio.
  - Standard di prestazione (serie 1200): si applicano alla esecuzione del lavoro assegnato, ad esempio pianificazione e supervisione, individuazione dello scopo, rischio e materialità, mobilitazione delle risorse, supervisione e gestione delle assegnazioni, evidenza di audit e assurance, nonché applicazione del giudizio professionale e della dovuta attenzione
  - Standard di reporting (serie 1400): riguardano i tipi di report, i mezzi di comunicazione e le informazioni comunicate
- **Linee guida**, a sostegno degli standard e divise in tre categorie:
  - Linee guida generali (serie 2000)
  - Linee guida attinenti le prestazioni (serie 2200)
  - Linee guida attinenti il reporting (serie 2400)
- **Strumenti e tecniche**, linee guida aggiuntive destinate ai revisori di Sistemi Informativi, ad esempio white paper, programmi di audit e assurance, nonché la famiglia di prodotti COBIT® 5

Un glossario online dei termini utilizzati in ITAF è disponibile all'indirizzo *www.isaca.org/glossary*.

Declinazione di responsabilità: le linee guida ISACA definiscono il livello minimo di prestazioni accettabili necessario per soddisfare le responsabilità previste dal Codice di etica professionale di ISACA. ISACA non asserisce in alcun modo che l'uso del prodotto garantirà esiti soddisfacenti. La presente pubblicazione non può essere considerata inclusiva di ogni procedura o test appropriato, né esclusiva di altri test o procedure, intesi a ottenere ragionevolmente gli stessi risultati. Nel determinare l'idoneità di una procedura o test specifico, i professionisti di audit sono tenuti ad applicare il loro giudizio professionale alle specifiche circostanze di controllo di un determinato sistema o ambiente IS.

Il Professional Standards and Career Management Committee (PSCMC) di ISACA offre servizi di consulenza per la definizione degli standard e delle linee guida. Prima della pubblicazione di qualsiasi documento, viene rilasciata a livello internazionale una bozza per aprire il dibattito pubblico. I commenti possono anche essere inviati al direttore dello sviluppo degli standard professionali all'indirizzo e-mail *standards@isaca.org*, fax (+1.847. 253.1443) o all'indirizzo di posta ordinaria ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA.

Standard di audit e assurance IS 1205 Evidenza

Dichiarazioni

1205.1 I revisori di Sistemi Informativi devono ottenere evidenze sufficienti ed appropriate per giungere a conclusioni ragionevoli su cui basare i risultati dell'incarico.

1205.2 I revisori di Sistemi Informativi devono valutare la sufficienza delle evidenze ottenute a sostegno delle conclusioni e per il conseguimento degli obiettivi dell'incarico.

Aspetti chiave

Nel portare a termine un incarico, i revisori di Sistemi Informativi devono:

- Ottenere evidenze appropriate e sufficienti, tra cui:
  - Procedure nelle modalità di esecuzione
  - Risultati prodotti da procedure eseguite
  - Documenti originali (in formato sia elettronico che cartaceo), registrazioni e informazioni a sostegno dell'incarico
  - Eccezioni e risultati dell'incarico
  - Documentazione che accerti che il lavoro è stato eseguito in conformità alle leggi, ai regolamenti ed alle politiche vigenti
- Preparare la documentazione, che deve essere:
  - Conservata e disponibile per un determinato periodo di tempo in un formato conforme agli standard professionali ed ai criteri dell'organizzazione di audit o assurance, nonché alle leggi e alle normative applicabili
  - Protetta dalla modifica o divulgazione non autorizzata nel corso del suo ciclo di vita, dalla predisposizione alla conservazione
  - Smaltita alla fine del periodo di conservazione
- Considerare la sufficienza delle evidenze per supportare il livello valutato di rischio di controllo quando le evidenze sono ottenute da un test dei controlli.
- Identificare, catalogare e creare riferimenti alle evidenze.
- Considerare proprietà come la fonte, la natura (ad es., scritta, orale, visuale, elettronica) e l'autenticità (presenza di timbri e firme digitali o manuali) delle evidenze quando se ne valuta l'affidabilità.
- Considerare il metodo di raccolta prove più economico e rapido per soddisfare gli obiettivi e contenere il rischio dell'incarico. Tuttavia, le difficoltà o i costi non costituiscono un motivo valido per omettere una procedura necessaria.
- Selezionare le procedure più appropriate per la raccolta delle evidenze in relazione agli argomenti oggetto di audit (tempi, natura e giudizio professionale). Le procedure utilizzate per ottenere le evidenze comprendono:
  - Richiesta di informazioni e conferma
  - Riesecuzione
  - Ricalcolo
  - Calcolo
  - Procedure analitiche
  - Ispezione
  - Osservazione diretta
  - Altri metodi generalmente accettati
- Considerare la fonte e la natura di tutte le informazioni ottenute al fine di valutarne l'affidabilità e determinare gli ulteriori requisiti di verifica. In genere, l'affidabilità delle evidenze è maggiore quando dette evidenze sono:
  - Scritte anziché orali.
  - Ottenute da fonti indipendenti.

Aspetti chiave

continua

- Ottenute dal revisore piuttosto che fornite dall'ente sottoposto a audit
- Certificate da terze parti indipendenti
- Conservate da terze parti indipendenti
- Risultato dell'ispezione
- Risultato dell'osservazione

- Ottenere evidenze oggettive e sufficienti tali da permettere a terze parti indipendenti e qualificate di rieseguire i test ed ottenere gli stessi risultati giungendo pertanto alle medesime conclusioni.
- Ottenere evidenze commisurate alla materialità e al rischio stimato.
- Dare il giusto risalto all'accuratezza e alla completezza delle informazioni quando tali informazioni sono fornite dall'impresa e vengono utilizzate dal revisore IS per eseguire le procedure di audit.
- Rivelare qualsiasi situazione in cui non sia possibile ottenere evidenze sufficienti per permettere di comunicare adeguatamente i risultati dell'incarico di audit o assurance IS.
- Proteggere le evidenze dalla modifica e dall'accesso non autorizzato.
  - Conservare le evidenze dopo il completamento del lavoro di audit o assurance IS per un periodo di tempo conforme a quanto previsto da leggi e normative vigenti.

Termini

Termine	Definizione
Evidenza appropriata	Misura della qualità dell'evidenza
Evidenza sufficiente	La misura della quantità dell'evidenza; una evidenza che supporta tutte le problematiche attinenti la materialità relativa allo scopo e all'obiettivo dell'audit. Vedere evidenza.

Collegamento alle linee guida

Tipo	Titolo
Linea guida	2205 Evidenza

Data di entrata in vigore

Questo standard ISACA dovrà essere applicato a tutti gli incarichi di audit e assurance IS a partire dal 1 novembre 2013.