Standard di audit e assurance IS 1401 Reporting

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.

Dichiarazioni

1401.1 I revisori di Sistemi Informativi devono redigere un report per comunicare i risultati al completamento dell'incarico, che comprenda:

- **l'identificazione dell'impresa, dei destinatari ed eventuali limitazioni su contenuto e distribuzione**
- **lo scopo, gli obiettivi dell'incarico, il periodo di copertura e la natura, i tempi e l'estensione del lavoro svolto**
- **i risultati, le conclusioni e le raccomndazioni**
- **eventuali limitazioni delle qualifiche o sullo scopo che il revisore ha adottato rispetto all'incarico**
- **firma, data e distribuzione in base agli standard dell'organizzazione della funzione di audit o della lettera di incarico**

1401.2 I revisori di Sistemi Informativi devono garantire che i risultati illustrati nel report di audit siano sostenuti da evidenze sufficienti e appropriate.

Aspetti chiave

I revisori di Sistemi Informativi devono:

- Ottenere dichiarazioni scritte del soggetto verificato in cui vengono descritte in dettaglio le aree critiche dell'incarico, i problemi emersi e la relativa risoluzione, nonché le asserzioni del soggetto stesso.
- Stabilire che le dichiarazioni del soggetto verificato sono state firmate e datate da lui stesso per indicare il riconoscimento delle sue responsabilità rispetto all'incarico.
- Documentare e conservare nelle carte di lavoro le dichiarazioni ricevute durante l'incarico, sia scritte che orali. Per gli incarichi di attestazione, le dichiarazioni del soggetto verificato devono essere ottenute per iscritto al fine di ridurre possibili incomprensioni.
- Personalizzare la forma e il contenuto del report per supportare il tipo di incarico svolto, ad esempio:
  - Audit (diretto o attestazione)
  - Verifica (diretta o attestazione)
  - Procedure concordate.
- Descrivere le debolezze materiali o significative e il loro effetto sul conseguimento degli obiettivi dell'incarico nel report.
- Discutere la bozza del report con la direzione dell'area soggetta ad audit, prima della finalizzazione e del rilascio, includendo, ove applicabile, i commenti della direzione sui risultati, le conclusioni e le raccomandazioni nel report finale.
- Comunicare le debolezze materiali e le carenze più evidenti nell'ambiente di controllo ai responsabili della governance e, ove applicabile, all'autorità preposta e confermare nel report l'avvenuta comunicazione.
- Fare riferimento a eventuali report separati nel report finale.
- Comunicare alla direzione del soggetto verificato le carenze nei controlli interni ritenute meno di importanti ma più di irrilevanti. In questi casi, ai responsabili della governance o all'autorità preposta deve essere notificato che tali carenze nei controlli interni sono state comunicate alla direzione del soggetto verificato.
- Identificare gli standard applicati nello svolgimento dell'incarico e comunicare, ove applicabile, eventuali non conformità a tali standard.

Standard di audit e assurance IS 1401 Reporting

Termini

Termine	Definizione
Informazioni significative	Nell'ambito dei controlli, comunicano al valutatore qualcosa di significativo sul funzionamento dei controlli sottostanti o dei relativi componenti. Informazioni che confermano direttamente il funzionamento dei controlli sono maggiormente significative. Anche le informazioni correlate indirettamente al funzionamento dei controlli possono essere significative, ma meno delle informazioni dirette. Fare riferimento agli obiettivi di qualità delle informazioni di COBIT 5
Informazioni affidabili	Informazioni accurate, verificabili e provenienti da una fonte oggettiva. Fare riferimento agli obiettivi di qualità delle informazioni di COBIT 5
Informazioni sufficienti	Le informazioni sono sufficienti quando i valutatori ne hanno raccolto un numero sufficiente per giungere a una conclusione ragionevole. Perché le informazioni possano essere ritenute sufficienti, tuttavia, devono innanzitutto essere idonee. Fare riferimento agli obiettivi di qualità delle informazioni di COBIT 5
Informazioni idonee	Informazioni significative (adeguate per conseguire l'obiettivo fissato), affidabili (accurate, verificabili e provenienti da una fonte oggettiva) e tempestive (prodotte e utilizzate nei tempi previsti). Fare riferimento agli obiettivi di qualità delle informazioni di COBIT 5
Informazioni tempestive	Prodotte e utilizzate nei tempi previsti per prevenire o individuare carenze nei controlli prima che diventino materiali per un'impresa. Fare riferimento agli obiettivi di qualità delle informazioni di COBIT 5

Collegamento agli standard e alle linee guida

Tipo	Titolo
Linea guida	2401 Reporting

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.