Standard di audit e assurance IS 1008 Criteri

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

1008.1 I revisori di Sistemi Informativi devono selezionare criteri, sulla cui base verrà valutato l'argomento, che siano oggettivi, completi, significativi, misurabili, comprensibili, ampiamente riconosciuti, autorevoli e compresi da o disponibili a tutti i lettori e utenti del report.

1008.2 I revisori di Sistemi Informativi devono valutare l'origine dei criteri e far convergere l'attenzione su quelli definiti da importanti enti autorevoli prima di accettarne di meno noti.

Aspetti chiave

I revisori di Sistemi Informativi devono:

- Considerare con attenzione la selezione di Criteri ed essere in grado di motivarla.
- Usare il giudizio professionale per garantire che l'applicazione dei criteri consentirà lo sviluppo di una conclusione o di un'opinione oggettiva ed equa non fuorviante per il lettore o l'utente. È riconosciuto che la direzione potrebbe definire criteri che non soddisfano tutti i requisiti.
- Considerare l'idoneità e la disponibilità dei criteri nel determinare i requisiti dell'incarico.
- Qualora i criteri non siano disponibili, siano incompleti o diversamente interpretabili, includere una descrizione e qualsiasi altra informazione necessaria a garantire che il report sia equo, oggettivo e comprensibile e che il contesto in cui si applicano i criteri sia incluso nel report.

L'idoneità e l'adeguatezza dei criteri di valutazione dell'argomento devono essere valutate in base ai cinque criteri di idoneità seguenti:

- **Oggettività:** i criteri non devono dare adito ad ambiguità che potrebbero influire negativamente sui risultati e sulle conclusioni e quindi trarre in inganno l'utente del report.
- **Completezza:** i criteri devono essere sufficientemente completi affinché tutti quelli che potrebbero influire sulle conclusioni del revisore sull'argomento possano essere identificati e utilizzati nello svolgimento dell'incarico di audit e assurance IS.
- **Pertinenza:** i criteri devono essere pertinenti all'argomento e contribuire ai risultati e alle conclusioni che soddisfano gli obiettivi dell'incarico di audit o assurance IS.
- **Misurabilità:** i criteri devono consentire una efficace misurazione dell'ambito di analisi e lo sviluppo di conclusioni coerenti se applicati da professionisti diversi in circostanze simili.
- **Comprensibilità:** i criteri devono essere comunicati chiaramente per non essere oggetto di interpretazioni sostanzialmente diverse da parte degli utenti.

L'accettabilità dei criteri dipende dalla disponibilità degli stessi ai destinatari del report, affinché tali utenti comprendano su quali basi sono state svolte le attività di assurance e la pertinenza dei rilievi e delle conclusioni. Fra le fonti si possono considerare quelle che sono:

- **Riconosciute:** i criteri devono essere sufficientemente riconosciuti affinché la loro applicazione non venga contestata dagli utenti.
- **Autorevoli:** i criteri devono riflettere le indicazioni di autorevoli fonti del settore

Aspetti chiave Continua

e risultare appropriati per l'argomento. Per fonti autorevoli si intendono gli enti professionali, i gruppi di settore, gli enti governativi e i legislatori.

- **Disponibili pubblicamente:** i criteri devono essere disponibili agli utenti del report. Per esempio gli standard sviluppati da enti che operano nel settore dell'auditing e della contabilità quali ISACA, l'International Federation of Accountants (IFAC) e altre istituzioni professionali o governative riconosciute.
- **Disponibili a tutti gli utenti:** ove non siano pubblicamente disponibili, i criteri devono essere comunicati a tutti gli utenti attraverso principi espressamente inclusi nel report. I principi sono dichiarazioni sull'argomento che soddisfano i requisiti di criteri appropriati affinché possano essere oggetto di audit.

Oltre all'idoneità e alla disponibilità, la selezione dei criteri di assurance IS dovrebbe anche considerare la fonte, in termini della loro applicazione e dei potenziali destinatari. Per esempio, nell'ambito della legislazione statale, i criteri derivanti dai principi sviluppati sulla base delle leggi e delle normative attinenti all'argomento dovrebbero essere i più appropriati. In altri casi, potrebbero essere maggiormente attinenti i criteri definiti dalle associazioni di categoria. Le possibili fonti dei criteri, elencate in ordine di importanza, sono:

- **Criteri definiti da ISACA:** criteri e standard disponibili pubblicamente che sono stati oggetto di una revisione e di un accurato processo di due diligence da parte di esperti di IT governance, controllo, sicurezza e assurance riconosciuti a livello internazionale.
- **Criteri definiti da altre organizzazioni di esperti:** analogamente ai criteri e agli standard ISACA, questi criteri attinenti all'argomento sono stati sviluppati, rivisti e sottoposti a un accurato processo di due diligence da parte di esperti di svariati settori.
- **Criteri definiti da leggi e normative:** sebbene le leggi e le normative possano costituire la base per la definizione di determinati criteri, la loro applicazione richiede un'estrema attenzione. Spesso, la stesura è molto complessa con specifici risvolti legali. In molti casi, potrebbe essere necessario rielaborare i requisiti come principi. Inoltre, l'espressione di un'opinione sulla legislazione è in genere limitata ai membri della professione legale.
- **Criteri definiti da imprese che non seguono un processo di validazione:** sono inclusi i criteri pertinenti sviluppati da altre imprese che non hanno seguito un processo di validazione e non sono stati oggetto di dibattito o consultazione pubblica.
- **Criteri sviluppati in modo specifico per l'incarico di audit o assurance IS**: anche se i criteri sviluppati in modo specifico per l'incarico di audit o assurance IS possono essere ritenuti appropriati, è necessario prestare un'attenzione particolare per garantire che questi criteri soddisfino i criteri di idoneità, in particolare la completezza, la misurabilità e l'oggettività. I criteri sviluppati in modo specifico per l'incarico di audit o assurance IS vengono espressi in forma di principi.

I criteri di selezione devono essere considerati in modo accurato. Sebbene la conformità alle leggi e normative locali sia fondamentale tanto da essere considerata un requisito obbligatorio, è riconosciuto che molti incarichi di audit e assurance IS comprendono aree, quali la gestione delle modifiche, i controlli generali IT e i controlli dell'accesso, che non sono considerate in leggi o normative. Inoltre, in alcuni settori, ad esempio il settore delle carte di credito e debito, sono stati definiti requisiti obbligatori che

devono essere soddisfatti. Laddove i requisiti legislativi siano basati su principi, il professionista deve assicurarsi che i criteri selezionati soddisfino gli obiettivi dell'incarico.

Durante lo svolgimento dell'incarico, è possibile che la disponibilità di maggiori informazioni renda evidente che alcuni criteri non sono più necessari per il conseguimento degli obiettivi. In queste circostanze, non sarà più necessario altro lavoro correlato ai criteri.

Termini

Termine	Definizione
Criteri	Standard e riferimenti, utilizzati per misurare e presentare l'argomento e utilizzati dall'auditor per valutare l'argomento. I criteri devono essere: • Oggettivi, privi di ambiguità • Completi, includere tutti i fattori pertinenti per raggiungere una conclusione • Pertinenti, correlati all'argomento • Misurabili, valutabili in modo coerente In un incarico di attestazione, si possono effettuare delle comparazioni con altri criteri per valutare i principi scritti dalla direzione sull'argomento. Il professionista giunge a una conclusione riguardante l'argomento facendo riferimento a criteri appropriati.

Collegamento alle linee guida

Tipo	Titolo
Linea guida	2008 Criteri

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.

