

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<sup>®</sup> 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<sup>®</sup> (Certified Information Systems Auditor<sup>®</sup>) 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*<sup>™</sup> 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<sup>®</sup> 5

Un glossario online dei termini utilizzati in ITAF è disponibile all'indirizzo [www.isaca.org/glossary](http://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](mailto: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.

**ISACA 2012-2013 Professional Standards and Career Management Committee**

<b>Steven E. Sizemore, CISA, CIA, CGAP, Chairperson</b>	<b>Texas Health and Human Services Commission, USA</b>
<b>Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP</b>	<b>HP Enterprises Security Services, UK</b>
<b>Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA</b>	<b>Myers and Stauffer LC, USA</b>
<b>Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP</b>	<b>British American Tobacco IT Services, Malaysia</b>
<b>Alisdair McKenzie, CISA, CISSP, ITCP</b>	<b>IS Assurance Services, New Zealand</b>
<b>Katsumi Sakagawa, CISA, CRISC, PMP</b>	<b>JIEC Co. Ltd., Japan</b>
<b>Ian Sanderson, CISA, CRISC, FCA</b>	<b>NATO, Belgium</b>
<b>Timothy Smith, CISA, CISSP, CPA</b>	<b>LPL Financial, USA</b>
<b>Rodolfo Szuster, CISA, CA, CBA, CIA</b>	<b>Tarshop S.A., Argentina</b>

## Standard di audit e assurance IS 1203 Prestazioni e supervisione

### Dichiarazioni

- 1203.1** I revisori di Sistemi Informativi devono svolgere il lavoro sulla base del piano di audit IS approvato per coprire il rischio identificato e in base alla pianificazione concordata.
- 1203.2** I revisori di Sistemi Informativi devono svolgere l'attività di supervisione sul personale di audit IS sul quale hanno la responsabilità di supervisione, in modo da conseguire gli obiettivi di audit e soddisfare gli standard di audit professionali applicabili.
- 1203.3** I revisori di Sistemi Informativi devono accettare solo quei compiti che rientrano nelle loro competenze o per cui si aspettino ragionevolmente o di poter acquisire le competenze durante l'incarico o di svolgerlo sotto supervisione.
- 1203.4** I revisori di Sistemi Informativi devono raccogliere evidenze sufficienti e appropriate per conseguire gli obiettivi di audit. Le conclusioni e i risultati dell'audit devono essere supportati da un'adeguata analisi e dalla corretta interpretazione di tali evidenze.
- 1203.5** I revisori di Sistemi Informativi devono documentare il processo di audit, descrivendo il lavoro e le evidenze a supporto dei risultati e delle conclusioni.
- 1203.6** I revisori di Sistemi Informativi devono argomentare le proprie conclusioni sulla base delle evidenze riscontrate.
- 

### Aspetti chiave

I revisori di Sistemi Informativi devono:

- Assegnare, con riferimento al tipo di incarico, le diverse attività ai membri del gruppo in base alle loro competenze e alla loro esperienza.
- Integrare il gruppo di audit IS con risorse esterne, ove opportuno, e assicurarsi che il loro lavoro venga accuratamente supervisionato.
- Gestire i ruoli e le responsabilità dei membri del gruppo di audit IS per tutta la durata dell'incarico, gestendo come minimo:
  - i ruoli di esecuzione e verifica
  - le responsabilità inerenti la definizione della metodologia e dell'approccio da adottare
  - la creazione di programmi di audit o assurance
  - lo svolgimento del lavoro
  - le problematiche che si presentano
  - la documentazione e l'illustrazione dei risultati
  - la stesura del report
- Far riesaminare ogni attività dell'incarico svolta da un membro del gruppo ad un altro membro.
- Utilizzare la migliore evidenza di audit ottenibile. Tale evidenza deve essere coerente con l'importanza dell'obiettivo di audit e il tempo e l'impegno necessari per ottenerla.
- Ottenere ulteriori evidenze se, in base al giudizio professionale, l'evidenza ottenuta non è sufficiente e appropriata per formare un'opinione o supportare i risultati e le conclusioni.

## Standard di audit e assurance IS 1203 Prestazioni e supervisione

- Aspetti chiave
- continua
- Organizzare e documentare il lavoro svolto durante l'incarico, seguendo procedure predefinite, approvate e documentate.
  - Includere nella documentazione:
    - obiettivi di audit e scopo del lavoro, programma di audit, passaggi eseguiti, evidenze raccolte, risultati, conclusioni e consigli
    - un numero di dettagli sufficiente per consentire ad una persona informata e diligente di rieseguire le attività svolte durante l'incarico e giungere alla stessa conclusione
    - identificazione degli esecutori delle attività e dei relativi ruoli nella preparazione e revisione della documentazione
    - la data di preparazione e revisione della documentazione
  - Ottenere una chiara, dettagliata e pertinente rappresentazione delle aree critiche dell'incarico, dei problemi emersi e della loro risoluzione, scritta dal soggetto verificato e contenente le dichiarazioni del soggetto stesso.
  - Assicurarsi che le dichiarazioni del soggetto controllato siano state firmate e datate per confermare il riconoscimento delle sue responsabilità rispetto all'incarico.
  - Documentare e conservare fra le carte di lavoro eventuali dichiarazioni ricevute durante l'incarico, sia scritte che orali.
- 

Collegamento agli standard e alle linee guida

Tipo	Titolo
Standard	1005 Diligenza professionale
Standard	1205 Evidenza
Standard	1401 Reporting
Linea guida	2202 Valutazione dei rischi durante la pianificazione

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.