

## Standard di audit e assurance IS 1207 Irregolarità e atti illeciti

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.

<b>ISACA 2012-2013 Professional Standards and Career Management Committee</b>	
<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 1207 Irregolarità e atti illeciti

### Dichiarazioni

- 1207.1** I revisori di Sistemi Informativi devono considerare il rischio di irregolarità e atti illeciti durante l'incarico.
- 1207.2** I revisori di Sistemi Informativi devono mantenere un atteggiamento di scetticismo professionale durante l'incarico.
- 1207.3** I revisori di Sistemi Informativi devono documentare e comunicare a tempo debito eventuali irregolarità materiali o atti illeciti alla parte appropriata.
- 

### Aspetti chiave

I revisori di Sistemi Informativi devono:

- Ridurre il rischio di audit a un livello accettabile durante la pianificazione e lo svolgimento dell'incarico:
  - Riconoscendo che gli errori materiali, le carenze nei controlli o le dichiarazioni errate dovute a irregolarità e atti illeciti potrebbero esistere, a prescindere dalla valutazione del rischio di irregolarità e di atti illeciti
  - Comprendendo l'impresa e il suo ambiente, compresi i controlli interni che hanno lo scopo di prevenire o individuare irregolarità e atti illeciti rilevanti per l'argomento, lo scopo e gli obiettivi dell'incarico
  - Ottenendo evidenze sufficienti e appropriate per determinare se la direzione o altri membri dell'organizzazione siano o meno a conoscenza di eventuali irregolarità e atti illeciti, siano essi reali, presunti o sospetti.
- Considerare relazioni insolite o impreviste che potrebbero indicare un rischio di errori materiali, carenze nei controlli o dichiarazioni errate dovute a irregolarità e atti illeciti durante lo svolgimento delle procedure di audit.
- Mettere a punto ed eseguire procedure per testare l'idoneità dei controlli interni e il rischio che la direzione ignori tali controlli intesi a prevenire o a individuare irregolarità e atti illeciti.
- Stabilire se gli errori identificati, le carenze nei controlli o le dichiarazioni errate possono indicare eventuali irregolarità o atti illeciti. In presenza di tale indicazione, considerare le implicazioni in relazione ad altri aspetti dell'incarico e, in particolare, alle dichiarazioni della direzione.
- Ottenere una dichiarazione scritta dalla direzione almeno una volta all'anno in base all'incarico per:
  - Riconoscere la responsabilità della direzione di predisporre ed implementare controlli interni intesi a prevenire e a individuare irregolarità e atti illeciti.
  - Divulgare i risultati pertinenti delle valutazioni dei rischi che indicano che gli errori, le carenze nei controlli o le dichiarazioni errate potrebbero essere la conseguenza di un'irregolarità o di un atto illecito.
  - Rendere nota la consapevolezza della direzione di irregolarità e atti illeciti riguardanti l'impresa in relazione alla direzione e ai dipendenti che rivestono ruoli significativi nel controllo interno.
  - Rendere nota la consapevolezza della direzione di eventuali irregolarità e atti illeciti sospetti o presunti che riguardano l'impresa secondo quanto comunicato da dipendenti, ex-dipendenti, regolatori e altri.
- Comunicare tempestivamente:
  - al livello appropriato della direzione eventuali informazioni identificate o ottenute che indicano la presenza di un'irregolarità o di un atto illecito

## Standard di audit e assurance IS 1207 Irregolarità e atti illeciti

Aspetti chiave continua	<p>materiale</p> <ul style="list-style-type: none"> <li>- ai responsabili della governance, eventuali irregolarità materiali e atti illeciti riguardanti la direzione o i dipendenti che rivestono ruoli significativi nel controllo interno</li> </ul> <ul style="list-style-type: none"> <li>• Comunicare ai responsabili della governance, eventuali debolezze materiali nella concezione e nell'implementazione dei controlli interni intesi a prevenire e a individuare eventuali irregolarità e atti illeciti identificati durante l'incarico, anche se non rientrano nello scopo.</li> <li>• Considerare i requisiti di reporting legali e professionali applicabili nelle specifiche circostanze.</li> <li>• Considerare il ritiro dall'incarico qualora errori materiali, carenze nei controlli, dichiarazioni errate o atti illeciti incidano continuamente sulle prestazioni dell'incarico.</li> <li>• Documentare tutte le comunicazioni, la pianificazione, i risultati, le valutazioni e le conclusioni associate a irregolarità materiali e atti illeciti segnalati alla direzione, ai responsabili della governance, ai regolatori e ad altri.</li> </ul>
-------------------------	---

Termini

Termine	Definizione
Irregolarità	Violazione di un requisito normativo o di un criterio di gestione definito. Può trattarsi di dichiarazioni errate intenzionali o di omissioni di informazioni relative ad atti illeciti non intenzionali o a gravi atti di negligenza riguardanti l'area oggetto di audit o l'impresa nel suo complesso.
Dichiarazione errata materiale	Falsa dichiarazione intenzionale o involontaria che attiene i risultati di un audit fino a un certo limite misurabile.
Scetticismo professionale	Attitudine che implica una certa capacità di ragionamento e una valutazione critica dell'evidenza di audit. Fonte: American Institute of Certified Public Accountants (AICPA) AU 230.07.

Collegamento agli standard e alle linee guida

Tipo	Titolo
Standard	1008 Criteri
Standard	1202 Valutazione dei rischi durante la pianificazione
Standard	1205 Evidenza
Linea guida	2206 Uso del lavoro di altri esperti
Linea guida	2207 Irregolarità ed atti illeciti

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.