

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 1201 Pianificazione dell'incarico

### Dichiarazioni

**1201.1** I revisori di Sistemi Informativi devono pianificare ciascun incarico di audit e assurance IS tenendo conto di:

- **Obiettivo(i), scopo, tempi e risultati da pubblicare**
- **Conformità alle leggi applicabili e agli standard di auditing professionali**
- **Uso di un approccio basato sui rischi, ove appropriato**
- **Problemi specifici dell'incarico**
- **Requisiti della documentazione e dei report**

**1201.2** I revisori di Sistemi Informativi devono sviluppare e documentare un piano di progetto per l'incarico di audit o assurance IS, in cui descrivere:

- **la natura, gli obiettivi, i tempi e i requisiti delle risorse per l'incarico**
  - **i tempi e la copertura delle procedure di audit per portare a termine l'incarico**
- 

### Aspetti chiave

I revisori di Sistemi Informativi devono:

- Conseguire una chiara comprensione dell'attività oggetto di audit. La vastità della conoscenza richiesta deve essere determinata in base alla natura dell'impresa, all'ambiente, ai rischi e agli obiettivi dell'incarico.
- Valutare le linee guida sull'argomento, secondo quanto stabilito dalle leggi, le normative, le regole, le direttive e le linee guida definite a livello governativo o di settore.
- Eseguire una valutazione dei rischi per garantire ragionevolmente che durante l'incarico tutti gli elementi materiali verranno adeguatamente coperti. Successivamente sarà possibile sviluppare strategie di auditing, livelli di materialità e requisiti delle risorse.
- Sviluppare il piano di progetto dell'incarico utilizzando metodologie di project management appropriate per assicurarsi che le attività vengano svolte nel rispetto dei tempi e del budget.
- Inserire nel piano le problematiche specifiche dell'assegnazione, ad esempio:
  - Disponibilità delle risorse con conoscenze, competenze ed esperienza appropriate
  - Identificazione degli strumenti necessari per raccogliere evidenze, eseguire test, nonché preparare e riepilogare le informazioni da includere nei report
  - Criteri di valutazione da utilizzare
  - Requisiti di reporting e distribuzione
- Documentare il piano di progetto dell'incarico di audit o assurance IS per indicare chiaramente:
  - Obiettivi, scopo e tempi
  - Risorse
  - Ruoli e responsabilità
  - Aree di rischio identificate e il relativo impatto sul piano dell'incarico
  - Strumenti e tecniche da utilizzare
  - Colloqui conoscitivi da condurre
  - Informazioni significative da ottenere
  - Procedure per verificare o convalidare le informazioni ottenute e il relativo utilizzo come evidenza
  - Le ipotesi assunte per quanto attiene l'approccio, la metodologia, le procedure, le conclusioni e i risultati anticipati

## Standard di audit e assurance IS 1201 Pianificazione dell'incarico

- Aspetti chiave
- Continua
- Pianificare per quanto possibile l'incarico relativamente ai tempi, alla disponibilità e ad altri impegni e requisiti della direzione e del soggetto verificato.
  - Rettificare il piano di progetto durante lo svolgimento dell'incarico di audit o assurance IS per risolvere problemi quali nuovi rischi, ipotesi di lavoro errate o risultati ottenuti con procedure già concluse.
  - Per gli incarichi interni:
    - Comunicare l'organizzazione della funzione di audit al soggetto verificato. Ove necessario, ricorrere a una lettera di incarico o a un documento equivalente per chiarire o confermare ulteriormente il coinvolgimento in incarichi specifici.
    - Comunicare il piano al soggetto verificato per informarlo adeguatamente e per consentirgli di fornire l'accesso alle persone, ai documenti e ad altre risorse, ove ritenuto necessario.
  - Per gli incarichi esterni:
    - Preparare una lettera separata per ogni incarico di audit e assurance IS esterno.
    - Preparare un piano di progetto per ogni incarico di audit e assurance IS esterno. Il piano deve almeno documentare gli obiettivi e lo scopo dell'incarico.
- 

Collegamento alle linee guida

Tipo	Titolo
Linea guida	2201 Pianificazione dell'incarico

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.