

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.

ISACA 2012-2013 Professional Standards and Career Management Committee	
Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, UK
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
Murari Kalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, New Zealand
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgium
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentina

Standard 1204 Materialità

Dichiarazioni

- 1204.1** Nella pianificazione di un incarico i revisori di Sistemi Informativi devono prendere in considerazione le potenziali debolezze o carenze nei controlli e stabilire se tali vulnerabilità possono causare una grave mancanza o una debolezza materiale.
- 1204.2** I revisori di Sistemi Informativi devono prendere in considerazione la materialità e il suo rapporto con il rischio di audit, determinando al contempo la natura, i tempi e la copertura delle procedure di audit.
- 1204.3** I revisori di Sistemi Informativi devono considerare l'effetto cumulativo delle debolezze o delle carenze nei controlli minori e stabilire se tali carenze si traducono in una grave mancanza o in una debolezza materiale.
- 1204.4** I revisori di Sistemi Informativi devono indicare nel report quanto segue:
- l'assenza di controlli o controlli inefficaci
 - la rilevanza delle carenze nei controlli
 - la probabilità che tali vulnerabilità comportino una grave mancanza o in una debolezza materiale
-

Aspetti chiave

Nel portare a termine un incarico, i revisori di Sistemi Informativi devono:

- Applicare il concetto di materialità a:
 - Pianificazione e svolgimento dell'incarico
 - Valutazione dell'effetto di aspetti, processi, controlli o errori specifici
 - Eventuali carenze, debolezze o la mancanza di politiche, procedure e controlli adeguati devono essere giudicati nelle circostanze specifiche dell'incarico.
 - Considerare le definizioni di materialità ove fornite dalle autorità legislative o regolamentari.
 - Prestare attenzione al fatto che la valutazione di materialità e di rischio di audit può variare a seconda delle circostanze e dei diversi ambienti.
 - Cercare di ridurre il rischio di audit a un livello accettabile e di soddisfare gli obiettivi durante la pianificazione e lo svolgimento dell'incarico.
 - Considerare la Materialità nel determinare la natura, i tempi e la copertura delle procedure di audit.
 - Ridurre il rischio di audit per le aree caratterizzate da una maggiore materialità estendendo il test dei controlli (ridurre il rischio di controllo) e/o le procedure dei test sostanziali (ridurre il rischio di non individuazione).
 - Valutare l'effetto dei controlli compensativi e stabilire se tali controlli sono efficaci nel determinare se una o più carenze nei controlli possono tradursi in una debolezza materiale.
 - Considerare l'effetto cumulativo di più errori o controlli inefficaci nel determinare la materialità.
 - Considerare non solo le dimensioni, ma anche la natura delle carenze nei controlli e le particolari circostanze in cui si sono verificate nel valutare il loro effetto complessivo sull'opinione o la conclusione dell'audit.
-

Standard 1204 Materialità

Termini

Termine	Definizione
Rischio di audit	<p>Il rischio di giungere a una conclusione errata in base ai risultati dell'audit. I tre componenti del rischio di audit sono:</p> <ul style="list-style-type: none"> • Rischio di controllo • Rischio di non individuazione • Rischio intrinseco
Vulnerabilità materiale	<p>Una carenza o una combinazione di più carenze nei controlli interni, tale che vi sia una ragionevole probabilità che un errore significativo non sia intercettato o tempestivamente rilevato.</p> <p>La carenza nei controlli è considerata materiale quando impedisce di acquisire una ragionevole certezza sul conseguimento degli obiettivi di controllo. Classificare una debolezza come materiale implica che:</p> <ul style="list-style-type: none"> • I controlli non sono stati istituiti e/o non vengono effettuati e/o sono inadeguati • deve esserci una fase di escalation <p>Sussiste un rapporto inverso tra materialità e livello di accettabilità del rischio di audit da parte del revisore IS. In altri termini, all'aumentare del livello di materialità diminuisce l'accettabilità del rischio di audit e <i>viceversa</i>.</p>
Materialità	<p>Concetto di audit riguardante l'importanza di un'informazione relativamente al suo impatto o effetto sul funzionamento dell'entità oggetto di audit. Espressione dell'importanza relativa di un argomento nel contesto dell'impresa considerata nel suo complesso.</p>

Collegamento agli standard e alle linee guida

Tipo	Titolo
Standard	1201 Pianificazione dell'incarico
Standard	1202 Valutazione dei rischi durante la pianificazione
Standard	1207 Irregolarità ed atti illeciti
Standard	1401 Reporting
Linea guida	2202 Valutazione dei rischi durante la pianificazione
Linea guida	2204 Materialità

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.