Standard di audit e assurance IS 1202 Valutazione dei rischi durante la pianificazione

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.

Standard di audit e assurance IS 1202 Valutazione dei rischi durante la pianificazione

Dichiarazioni

1202.1 **La funzione di audit e assurance dei Sistemi Informativi deve adottare un approccio alla valutazione dei rischi appropriato e una metodologia di supporto adeguata per sviluppare il piano di audit IS e determinare le priorità per un'allocazione efficace delle risorse di audit IS.**

1202.2 **Nell'ambito della pianificazione dei singoli incarichi, i revisori di Sistemi Informativi devono identificare e valutare i rischi associati all'area oggetto della verifica.**

1202.3 **I revisori di Sistemi Informativi devono prendere in considerazione i rischi associati all'argomento, il rischio di audit e l'esposizione correlata all'impresa.**

Aspetti chiave

Nel pianificare le attività in corso, la funzione di audit e assurance IS deve:

- Condurre e documentare, almeno annualmente, una valutazione dei rischi per facilitare lo sviluppo del piano di audit IS.
- Includere, nell'ambito della valutazione dei rischi, gli obiettivi e i piani strategici dell'organizzazione, nonché le iniziative e il modello di gestione dei rischi dell'impresa.
- Per ogni incarico di audit e assurance IS, quantificare e giustificare la quantità di risorse di audit IS necessarie per soddisfare i requisiti dell'incarico.
- Utilizzare le valutazioni dei rischi nella selezione di aree ed elementi di interesse per l'audit e nelle decisioni per definire e portare a termine incarichi di audit e assurance IS specifici.
- Richiedere l'approvazione della valutazione dei rischi alle figure preposte e ad altre parti interessate.
- Assegnare priorità e pianificare il lavoro di audit e assurance IS in base alle valutazioni dei rischi.
- In base alla valutazione dei rischi, sviluppare un piano che:
  - Funga da modello per le attività di audit e assurance IS
  - Prenda in considerazione i requisiti e le attività di audit e assurance non IS
  - Venga aggiornato almeno annualmente e approvato dai responsabili della governance
  - Affronti le responsabilità definite dall'organizzazione della funzione di audit

Quando pianificano un incarico, i revisori di Sistemi Informativi devono:

- Identificare e valutare i rischi associati all'area oggetto della verifica.
- Condurre una valutazione preliminare dei rischi associati all'area oggetto della verifica per ogni incarico. Gli obiettivi di ogni specifico incarico devono riflettere i risultati della valutazione dei rischi preliminare.
- Nel prendere in considerazione le aree di rischio e nel pianificare un incarico specifico, tenere presente gli audit, le verifiche e i risultati precedenti, incluse le attività correttive. Considerare inoltre il processo di valutazione dei rischi della Direzione.
- Tentare di ridurre il rischio di audit a un livello accettabile e di conseguire gli obiettivi attraverso una valutazione appropriata dell'argomento IS e dei controlli correlati, il tutto durante la pianificazione e l'esecuzione dell'audit IS.
- Quando si pianifica una procedura di audit IS specifica, riconoscere che più bassa

sarà la soglia di materialità, più precise saranno le aspettative di audit e maggiore il rischio associato all'audit.
- Per il ridurre il rischio di una materialità più alta, compensare estendendo il test dei controlli (ridurre il rischio di controllo) e/o le procedure di test sostanziali (ridurre il rischio di non individuazione) per ottenere una maggiore certezza.

Termini

Termine	Definizione
Organizzazione della funzione di audit	Documento approvato dai responsabili della governance che definisce lo scopo, l'autorità e la responsabilità dell'attività di audit interna. L'organizzazione della funzione di audit prevede: • l'individuazione della posizione della funzione di audit interna in seno all'impresa • l'autorizzazione dell'accesso a registrazioni e a proprietà personali e fisiche correlati alle prestazioni degli incarichi di audit e assurance IS • l'individuazione dello scopo delle attività della funzione di audit
Rischio di audit	Il rischio di giungere a una conclusione errata in base ai risultati dell'audit. I tre componenti del rischio di audit sono: • Rischio di controllo • Rischio di non individuazione • Rischio intrinseco
Rischio associato all'argomento oggetto di audit	Rischio associato all'area oggetto della verifica: • Rischio commerciale (solvenza del cliente, affidabilità creditizia, fattori di mercato e così via) • Rischio associato al contratto (responsabilità, prezzo, tipo, penali e così via) • Rischio associato al paese (contesto politico, ambiente, sicurezza e così via) • Rischio associato al progetto (risorse, competenze, metodologia, stabilità del prodotto e così via) • Rischio tecnologico (soluzione, architettura, rete dell'infrastruttura hardware e software, canali di distribuzione e così via) Vedere Rischio intrinseco.
Rischio di controllo	Il rischio che esista un errore materiale impossibile da individuare o prevenire puntualmente attraverso il sistema di controllo interno. (Vedere Rischio intrinseco.)
Rischio di non individuazione	Il rischio che le procedure dei test sostanziali adottate dal revisore IS non consentano l'individuazione di un errore che potrebbe essere materiale, da solo o in combinazione con altri errori. Vedere Rischio di audit.
Rischio intrinseco	L'esposizione o il livello di rischio senza prendere in considerazione le azioni che la direzione ha intrapreso o potrebbe

	intraprendere (implementazione dei controlli). Vedere Rischio di controllo.
Materialità	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 consideratanel suo complesso.
Valutazione dei rischi	Processo utilizzato per identificare e valutare il rischio e i suoi effetti potenziali. Le valutazioni dei rischi consentono di identificare gli aspetti o le aree che presentano il rischio, la vulnerabilità o l'esposizione più elevata per l'impresa per includerli nel piano di audit annuale IS. Le valutazioni dei rischi consentono inoltre di gestire la consegna del progetto e il rapporto rischio-benefici del progetto.
Test sostanziali	Ottenere evidenza di audit sulla completezza, l'accuratezza o l'esistenza di attività o transazioni durante il periodo di audit

Collegamento alle linee guida

Tipo	**Titolo**
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.