

La natura specialistica dell'audit dei sistemi informativi (SI) e competenze necessarie per condurlo richiedono standard specifici. Uno degli obiettivi dell'Information Systems Audit and Control Association® (ISACA®) consiste nel promuovere standard di applicazione globale che ne rispecchino la visione. Lo sviluppo e la disseminazione degli standard di audit SI rappresenta il contributo professionale dell'ISACA alla comunità dei revisori. La strutturazione degli standard di audit SI prevede livelli plurimi di adozione:

- Gli Standard definiscono i requisiti obbligatori di audit e di reporting. Indicano:
 - ai revisori SI il livello minimo accettabile di prestazioni necessario a soddisfare le responsabilità previste dal Codice di etica professionale ISACA;
 - ai dirigenti ed agli interessati, le aspettative della professione sull'operato degli addetti;
 - ed i requisiti ai detentori della Certified Information Systems Auditor® (CISA®). La mancata osservanza di tali standard può causare una investigazione sulla condotta del detentore della certificazione CISA da parte del consiglio direttivo dell'ISACA o dell'appropriato comitato ISACA e, in ultima istanza, misure disciplinari.
- Le Direttive regolano l'applicazione degli standard di audit SI. Il revisore SI deve prenderle in considerazione all'atto dell'implementazione degli standard, usare oculato giudizio nella loro applicazione ed essere in grado di giustificare qualsiasi eventuale deviazione. Le direttive di audit SI si propongono di chiarire le modalità di attuazione degli standard di audit SI.
- Le Procedure presentano esempi delle strategie applicabili dal revisore SI nel corso dell'audit. I documenti procedurali indicano come soddisfare gli standard nel corso del lavoro di revisione SI, ma non definiscono alcun requisito. Lo scopo delle procedure di audit SI consiste nel fornire ulteriori informazioni sull'osservanza degli standard di audit SI.

Le risorse COBIT® rappresentano la migliore fonte di informazioni sulla prassi di audit. COBIT *Framework* dichiara: "La direzione ha la responsabilità di salvaguardare tutti i beni dell'azienda. Per assolvere a tale responsabilità e soddisfare le aspettative, la direzione deve stabilire un sistema adeguato di controlli interni". COBIT offre un gruppo dettagliato di controlli e di tecniche di controllo, mirato all'ambiente di gestione dei sistemi informativi. La selezione del materiale COBIT più idoneo allo scopo di un dato audit dipende dalla scelta degli specifici processi COBIT IT e dall'impostazione dei criteri informativi COBIT.

Secondo la definizione di COBIT *Framework*, l'organizzazione di quanto segue fa parte del processo gestionale IT. COBIT è destinato ad essere usato dalla direzione IT e del business, oltre che dai revisori SI. Pertanto, il suo uso consente di comprendere gli obiettivi aziendali, di comunicare la prassi migliore e di avanzare suggerimenti rispecchianti standard di riferimento comunemente accettati. COBIT comprende:

- Obiettivi di controllo — Dichiarazioni generali particolareggiate e ad alto livello in merito al buon controllo minimo.
- Prassi di controllo — Motivazioni pratiche e procedure di implementazione degli obiettivi di controllo.
- Direttive di audit — Indicazioni guida relative a ciascuna area di controllo sulle metodiche di analisi conoscitiva, valutazione dei controlli e di conformità e quantificazione dei rischi associati alla mancata esecuzione dei controlli stessi.
- Direttive gestionali — Indicazioni guida su come valutare e migliorare il rendimento del processo IT, usando modelli di maturità, metriche e fattori critici di successo. Definiscono il quadro di riferimento, orientato alla direzione, dell'autovalutazione continua e proattiva dei controlli, specificatamente concentrato su:
 - Misurazione del rendimento — In che misura la funzione IT supporta i requisiti del business? Le direttive di gestione possono essere usate per supportare sia workshop di autovalutazione che l'implementazione da parte dei dirigenti delle procedure di monitoraggio e miglioramento permanente previste dallo schema di conduzione IT.
 - Definizione dei profili di controllo IT — Quali sono i processi IT più importanti? Quali sono i fattori critici di successo dei controlli?
 - Sensibilizzazione — Quali sono i rischi propri del mancato conseguimento degli obiettivi?
 - Valutazione comparativa (benchmarking) — Gli altri cosa fanno? Come si fa a paragonare e misurare i risultati? Le direttive gestionali forniscono esempi di metriche atte a valutare il rendimento IT in termini di business. Gli indicatori chiave degli obiettivi identificano e misurano gli esiti dei processi IT e gli indicatori chiave del rendimento valutano le prestazioni dei processi, misurandone gli abilitatori. I modelli e gli attributi di maturità permettono di eseguire il benchmarking e le valutazioni della capacità, permettendo ai dirigenti di misurare la capacità di controllo, identificare le carenze e definire le strategie di miglioramento.

Un Glossario dei termini è disponibile presso il sito Web della ISACA, www.isaca.org/glossary. I sostantivi audit e revisione sono sinonimi.

Esonero: Le indicazioni formulate dalla ISACA definiscono il livello minimo accettabile di prestazioni, necessario a soddisfare le responsabilità previste dal Codice di etica professionale ISACA. La ISACA non asserisce in alcun modo che l'osservanza di tali indicazioni garantisca esiti soddisfacenti. La presente pubblicazione non può essere considerata inclusiva di ogni procedura o test appropriati, né esclusiva di test o procedure diversi, volti ad ottenere in modo ragionato gli stessi risultati. Al momento di determinare l'idoneità di una procedura o test specifici, gli specialisti dei controlli devono esercitare il proprio giudizio professionale e valutare le specifiche circostanze presentate dal controllo di un dato sistema o ambiente informatico.

Il comitato di standardizzazione ISACA si è impegnato a condurre una vasta consultazione in preparazione del rilascio delle procedure, direttive e standard di audit SI. Prima della pubblicazione di alcun documento, il comitato di standardizzazione pubblica a livello internazionale le bozze divulgative, aprendo il dibattito al grande pubblico. Laddove necessario, il comitato di standardizzazione richiede il parere e la consulenza di quanti abbiano una speciale expertise o interesse in relazione all'argomento in discussione. Il comitato di standardizzazione conduce un programma permanente di sviluppo e dà il benvenuto all'input dei membri ISACA e dei terzi interessati, volto ad identificare le problematiche emergenti che richiedono nuovi standard. Gli eventuali suggerimenti possono essere inviati tramite e-mailed (standards@isaca.org), via fax (+1.847.253.1443) o per posta (l'indirizzo è riportato in calce al documento) alla sede ISACA International Headquarters, all'attenzione del direttore Ricerca, standard e rapporti con il mondo accademico. Questa pubblicazione ha visto le stampe il 1° luglio 2005.

Introduzione

- 01 Oltre ad offrire le opportune indicazioni, gli standard ISACA esprimono, riportandoli in neretto, i principi di base e le procedure essenziali che sono considerati obbligatori.
- 02 Questo standard ISACA si propone di definire le irregolarità e gli atti illeciti che il revisore SI deve prendere in considerazione durante il processo di audit.

Standard

- 03 Al momento di pianificare e svolgere l'audit e per mantenerne basso il livello di rischio, il revisore SI deve prendere in considerazione il rischio di irregolarità ed atti illeciti.
- 04 Il revisore SI deve mantenere un atteggiamento di scetticismo professionale durante l'audit, riconoscendo la possibilità di confrontarsi con false dichiarazioni materiali indotte da irregolarità o atti illeciti, indipendentemente dalla propria valutazione del rischio di tali irregolarità ed atti illeciti.
- 05 Il revisore SI deve maturare una buona comprensione dell'organizzazione e del suo ambiente, controlli interni compresi.
- 06 Il revisore SI deve ottenere prove di audit sufficienti ed atte a determinare se la direzione o altri membri dell'organizzazione siano o meno a conoscenza di qualsiasi irregolarità ed atto illecito, sia esso attuale, sospetto o presunto.
- 07 Al momento di condurre le procedure di audit, e al fine di conseguire una buona comprensione dell'organizzazione e del suo ambiente, il revisore SI deve prendere in considerazione rapporti interpersonali imprevisi o insoliti che possano indicare un rischio di false dichiarazioni materiali indotte da irregolarità ed atti illeciti.
- 08 Il revisore SI deve predisporre e svolgere procedure di verifica dell'adeguatezza dei controlli interni e del rischio di esclusione dei controlli da parte della direzione.
- 09 Al momento dell'identificazione di una falsa dichiarazione, il revisore SI deve valutare se si tratti o meno di un'irregolarità o di un atto illecito. In assenza di tale indicazione, il revisore SI deve considerare le implicazioni in relazione agli altri aspetti dell'audit, ed in particolare alle asserzioni della direzione.
- 10 Il revisore SI deve ottenere una dichiarazione scritta dalla direzione con frequenza almeno annuale, o più spesso, in base ai piani di audit. La direzione deve:
 - Riconoscere la propria responsabilità di predisporre ed implementare controlli interni atti ad evitare e rivelare le irregolarità e gli atti illeciti
 - Divulgare al revisore SI i risultati della valutazione del rischio di false dichiarazioni materiali indotte da irregolarità o atti illeciti
 - Divulgare al revisore SI la propria conoscenza di irregolarità o atti illeciti, in grado di influenzare l'organizzazione, relativi a:
 - Direzione
 - Dipendenti che svolgono ruoli significativi in termini di controlli interni
 - Divulgare al revisore SI la propria conoscenza di qualsiasi irregolarità o atto illecito presunto o sospetto che interessi l'organizzazione, comunicato da dipendenti, ex-dipendenti, enti regolamentatori ed altri
- 11 Se identifica una irregolarità materiale o un atto illecito, o ottiene informazioni in merito alla possibile esistenza di una irregolarità materiale o di un atto illecito, il revisore SI deve comunicare tempestivamente la cosa al livello direzionale responsabile.
- 12 Se identifica una irregolarità materiale o un atto illecito che riguarda la direzione o i dipendenti che svolgono ruoli significativi in termini di controlli interni, il revisore SI deve comunicare tempestivamente la cosa a chi è incaricato della gestione.
- 13 Il revisore SI deve informare il livello direzionale responsabile, e coloro che sono incaricati della gestione, in merito alle carenze materiali di progettazione ed implementazione dei controlli interni, al fine di evitare e rilevare le irregolarità e gli atti illeciti che possano essere emersi durante l'audit.
- 14 Se incontra circostanze eccezionali che ne coartano la capacità di continuare a svolgere l'audit a causa di una falsa dichiarazione materiale o di un atto illecito, il revisore SI deve considerare sia le responsabilità legali e professionali applicabili in tali circostanze, compresa l'esistenza o meno del requisito di notifica di quanti partecipino all'audit o in alcuni casi di chi è incaricato della gestione o detiene autorità regolamentatrici, che la possibile rinuncia all'incarico.
- 15 Il revisore SI deve documentare tutte le comunicazioni, pianificazione, risultati, valutazioni e conclusioni associate alle irregolarità materiali ed agli atti illeciti denunciati alla direzione, a coloro che sono incaricati della gestione, gli enti regolamentatori ed altri.

Commenti

- 16 Il revisore SI deve fare riferimento alla direttiva di audit SI G19, Irregolarità ed atti illeciti, per la definizione di ciò che costituisce una irregolarità ed atto illecito.
- 17 Il revisore SI deve ottenere garanzie ragionevoli in merito all'assenza di false dichiarazioni materiali indotte da irregolarità o atti illeciti. Nessun revisore SI può ottenere garanzie assolute determinate da fattori quali l'uso di giudizi soggettivi, la portata dei test e le limitazioni intrinseche dei controlli interni. Le prove di audit disponibili al revisore SI, durante un audit, dovrebbero avere carattere persuasivo piuttosto che conclusivo.
- 18 Il rischio di mancata rilevazione di una falsa dichiarazione materiale indotta da un atto illecito è maggiore di quello di mancata rilevazione di una falsa dichiarazione materiale indotta causata da una irregolarità o da un errore, visto che gli atti illeciti possono prevedere schemi complessi sviluppati per occultare o nascondere gli eventi o le false dichiarazioni intenzionali a lui rivolte.

- 19 L'esperienza precedente e la conoscenza dell'organizzazione maturate dal revisore SI dovrebbero assisterlo durante l'audit. Quando pone domande ed esegue le procedure di audit, il revisore SI non può ignorare completamente le esperienze passate, ma deve mantenere un certo livello di scetticismo professionale. Il revisore SI non deve ritenersi soddisfatto di prove di audit meno che persuasive sulla base della fiducia personale nell'onestà ed integrità della direzione e di coloro che sono incaricati della gestione. Il revisore SI ed il team di audit devono discutere la suscettibilità dell'organizzazione alle irregolarità ed agli atti illeciti, nel quadro del processo di pianificazione e durante l'intero svolgimento dell'audit.
- 20 Per valutare il rischio di irregolarità materiali e di atti illeciti, il revisore SI deve considerare l'uso delle:
- Proprie conoscenze ed esperienze precedenti con l'organizzazione (compresa l'esperienza in merito all'onestà ed all'integrità della direzione e di coloro che sono incaricati della gestione).
 - Informazioni ottenute ponendo domande in merito alla direzione.
 - Dichiarazioni dei manager e controfirme dei controlli interni
 - Altre informazioni affidabili raccolte durante l'audit
 - Valutazioni dei dirigenti in merito al rischio di irregolarità ed atti illeciti ed il processo da loro instaurato per identificare e rispondere a tale rischio
- 21 È opportuno fare riferimento alle seguenti indicazioni per conseguire ulteriori informazioni sulle irregolarità e gli atti illeciti:
- Direttiva di audit SI G5, Statuto di audit
 - Framework COBIT, obiettivi di controllo DS3, DS5, DS9, DS11 e PO6
 - Legge statunitense Sarbanes-Oxley del 2002
 - Legge statunitense sulla corruzione all'estero del 1977

Data di entrata in vigore

- 22 Questo standard di audit ISACA va applicato a tutti gli audit dei sistemi informativi a partire dal 1° settembre 2005.

Comitato sugli standard 2004-2005 • Information Systems Audit and Control Association	
Presidente, Sergio Fleginsky, CISA ICI Paints, Uruguay	
Svein Aldal Aldal Consulting, Norvegia	
John Beveridge, CISA, CISM, CFE, CGFM, CQA	Ufficio del Revisore dello stato del Massachusetts, USA
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP	Tangerine Consulting, Italia
Christina Ledesma, CISA, CISM	Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, PCP	Consiglio comunale di Brisbane, Australia
V. Meera, CISA, CISM, ACS, CWA	Microsoft Corporation, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Ikanos Communications., India
Peter Niblett, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Thomas Thompson, CISA	Ernst & Young, UAE

© Copyright 2005
 Information Systems Audit and Control Association
 3701 Algonquin Road, Suite 1010
 Rolling Meadows, IL 60008 USA
 Telefono: +847.253.1545
 Fax: +847.253.1443
 E-mail: standards@isaca.org
 Sito Web: www.isaca.org