



STANDARD DI AUDIT SI

STATUTO DI AUDIT

Documento n° S1

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 15 ottobre 2004.

Statuto di audit S1

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 Lo scopo di questo standard di audit SI consiste nello stabilire e fornire indicazioni in merito allo statuto di audit usato durante il processo di revisione.

Standard

- 03 Lo scopo, responsabilità, autorità e trasparenza della funzione di revisione dei sistemi informativi o degli incarichi di audit di tali sistemi devono essere opportunamente documentati in uno statuto di audit o lettera di impegnativa.**
- 04 Lo statuto di audit o lettera di impegnativa devono essere concordati ed approvati dal livello organizzativo appropriato.**

Commenti

- 05 Nel caso della funzione di revisione di sistemi informativi interni, lo statuto di audit va preparato per le attività in corso. Lo statuto di audit va sottoposto a revisione con scadenze annuali o più ravvicinate, qualora richiesto dalla modifica o variazione delle responsabilità. Una lettera di impegnativa può essere usata da un revisore SI interno per chiarire o confermare ulteriormente il suo coinvolgimento in compiti specifici di audit o meno. Per le revisioni SI esterne, una lettera di impegnativa va normalmente redatta per ciascun incarico di audit o meno.
- 06 Lo statuto di audit o la lettera di impegnativa devono essere particolareggiati quanto basta per comunicare lo scopo, la responsabilità ed i limiti della funzione o dell'incarico di audit.
- 07 Lo statuto di audit o la lettera di impegnativa devono essere rivisti periodicamente per garantire la buona documentazione dello scopo e delle responsabilità.
- 08 Per ulteriori informazioni sulla stesura di uno statuto di audit o lettera di impegnativa, fare riferimento alla seguente indicazione:
- Direttiva G5, Statuto di audit
 - COBIT *Framework*, obiettivo di controllo M4

Data di entrata in vigore

- 09 Questo standard ISACA va applicato a tutti gli audit dei sistemi informativi a partire dal 1° gennaio 2005.

Comitato sugli standard 2004-2005 • Information Systems Audit and Control Association

Chair, Sergio Fleginsky, CISA	PricewaterhouseCoopers, 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	Value Partners, Italia
Christina Ledesma, CISA, CISM	Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP	Consiglio Comunale di Brisbane, Australia
V. Meera, CISA, CISM, ACS, CISSP, CWA	Microsoft Corporation, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	NextLinx India Private Ltd., India
Peter Niblett, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, Australia
John G. Ott, CISA, CPA	Aetna Inc., USA
Thomas Thompson, CISA	Ernst & Young, UAE

© Copyright 2004
Information Systems Audit e Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telefono: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: standards@isaca.org
Sito Web: www.isaca.org