

## S16 E-COMMERCE

La natura specialistica dell'audit dei sistemi informativi (SI) e delle competenze necessarie per condurlo richiedono standard specifici. Uno degli obiettivi di ISACA<sup>®</sup> consiste nel promuovere standard applicabili a livello globale, in linea con la propria 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 manager ed agli interessati, le aspettative della professione sull'operato degli addetti; e
  - i requisiti ai detentori della designazione Certified Information Systems Auditor<sup>™</sup> (CISA<sup>®</sup>). 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.

**Control Objectives for Information and related Technology (COBIT<sup>®</sup>)** è uno strumento di supporto ed un framework di conduzione della tecnologia delle informazioni (IT) che permette ai manager di ovviare alle discrepanze tra requisiti di controllo, soluzioni tecniche e rischi di esercizio. COBIT permette un chiaro sviluppo delle politiche e l'instaurazione della buona prassi di controllo IT a tutti i livelli di una data organizzazione. Pone l'accento sulla conformità regolamentare, aiuta le organizzazioni ad accrescere il valore derivato da IT, permette l'allineamento e semplifica l'implementazione dei concetti del framework COBIT.

Essendo destinato ad essere usato dai manager commerciali ed IT, come pure dai revisori SI, consente di comprendere gli obiettivi aziendali, di comunicare la prassi migliore e di avanzare suggerimenti rispecchianti standard di riferimento comunemente accettati. COBIT è disponibile ai fini del download presso il sito Web della ISACA, [www.isaca.org/cobit](http://www.isaca.org/cobit). Come definito nel *framework* COBIT, ciascuno dei seguenti prodotti e/o elementi correlati è organizzato dal processo di gestione IT:

- Obiettivi di controllo — Dichiarazioni generiche di buon controllo minimo riferire ai processi IT
- Direttive di gestione — Indicazioni sulla valutazione ed il miglioramento della performance dei processi IT, usando modelli di maturità; schede RACI (Responsible, Accountable, Consulted, Informed); obiettivi e metriche. Definiscono il quadro di riferimento, orientato alla direzione, dell'autovalutazione continua e proattiva dei controlli, specificatamente concentrato su:
  - Misurazione della performance
  - Definizione del profilo dei controlli IT
  - Sensibilizzazione
  - Valutazione comparativa (benchmarking)
- *Pratiche di controllo COBIT* — Dichiarazioni di rischio e valori ed indicazioni sull'implementazione degli obiettivi di controllo
- *Guida alla garanzia IT* — 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

Un **glossario** dei termini è disponibile presso il sito Web della ISACA, [www.isaca.org/glossary](http://www.isaca.org/glossary). I termini audit e revisione sono usati in modo intercambiabile negli standard, direttive e procedure di audit SI.

**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 inoltrati tramite e-mail ([standards@isaca.org](mailto:standards@isaca.org)), via fax (+1 847.253.1443) o per posta (l'indirizzo è riportato in calce al documento) alla sede internazionale ISACA, all'attenzione del direttore degli standard di ricerca e delle relazioni accademiche. Questo materiale è stato rilasciato il 1 dicembre 2007.

## S16 E-commerce

### 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, assieme alle relative indicazioni guida.
- 02 Lo scopo di questo standard ISACA consiste nello stabilire e fornire indicazioni in merito alla revisione degli ambienti di commercio elettronico.

### Standard

- 03 Il revisore SI deve valutare i controlli del caso e i rischi al momento di rivedere gli ambienti di e-commerce, in modo da garantire che le transazioni di e-commerce siano opportunamente controllate.**

### Commenti

- 04 E-commerce è definito come l'insieme dei processi tramite i quali un'organizzazione è elettronicamente in relazione d'affari con i propri clienti, fornitori ed altri partner commerciali esterni, usando Internet quale tecnologia attuativa. Di conseguenza, comprende i modelli di commercio elettronico business-to-business (B2B o tra business) e business-to-consumer (B2C o tra business e clienti).
- 05 Il revisore SI deve far uso di una tecnica o approccio di valutazione dei rischi appropriati al momento di sviluppare il piano complessivo di audit SI. Ciò comprende la copertura degli ambienti di e-commerce.
- 06 Il revisore SI deve considerare l'uso di tecniche di analisi dei dati, compreso l'uso della garanzia continua, che permette ai revisori SI di monitorare di continuo l'affidabilità del sistema e di raccogliere prove selettive di audit usando il computer al momento di rivedere le attività di e-commerce.
- 07 Il livello di skill e conoscenze necessari per comprendere le implicazioni di controllo e di gestione dei rischi dell'e-commerce variano a seconda della complessità delle attività di commercio elettronico di una organizzazione.
- 08 Il revisore SI deve comprendere la natura e crucialità del processo di business supportato dall'applicazione di e-commerce prima di cominciare l'audit, in modo da permettere di valutare i risultati nell'appropriato contesto.
- 09 Per ulteriori informazioni sull'e-commerce, fare riferimento alle indicazioni successive:
- Direttiva G21 Revisione dei sistemi ERP (Enterprise Resource Planning)
  - Direttiva G22 Revisione dell'e-commerce Business-to-consumer (B2C)
  - Direttiva G24 Attività bancarie in Internet
  - Direttiva G25 Revisione delle reti VPN (Virtual Private Network)
  - Direttiva G33 Considerazioni generali sull'uso di Internet
  - Procedura P6 Firewall
  - Framework COBIT e obiettivi di controllo.

### Data di entrata in vigore

- 10 Questo standard ISACA viene applicato agli audit SI a partire dal primo febbraio 2008.

#### Comitato sugli standard ISACA 2007-2008

Chair Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Capco IT Services India Private Limited, India
Brad David Chin, CISA, CPA	Google Inc., USA
Sergio Fleginsky, CISA	ICI Paints, Uruguay
Maria Gonzalez, CISA	HomeLand Office, Spagna
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew MacLeod, CISA, CIA, FCPA, PCP	Consiglio comunale di Brisbane, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Jason Thompson, CISA, CIA	KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA

© 2007 ISACA. Tutti i diritti riservati.

ISACA  
3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Telefono: +847.253.1545  
Fax: +847.253.1443  
E-mail: [standards@isaca.org](mailto:standards@isaca.org)  
Sito Web: [www.isaca.org](http://www.isaca.org)